



**State of New Hampshire
Department of Health and Human Services**

**REQUEST FOR PROPOSALS
RFP-2022-DEHS-01-STATE
FOR**

State Disbursement Unit

April 8, 2021



TABLE OF CONTENTS

1. INTRODUCTION	4
1.1. Purpose and Overview	4
1.2. Contract Period	4
2. BACKGROUND	4
2.1. New Hampshire Department of Health and Human Services, DEHS	4
2.2. Background	4
2.3. SDU Audits	10
2.4. Disqualification	11
3. STATEMENT OF WORK	11
3.1. Scope of Services	11
3.2. Child Support Billing Services	12
3.3. Processing Payments Received	15
3.4. Disbursing Child Support Payments	20
3.5. Electronic Funds Transfer and Electronic Data Interchange Services (EFT/EDI)	21
3.6. Self-Service Web Portal	26
3.7. Automated Response Unit (ARU) for Child Support Payees	28
3.8. Customer Services for Child Support Payee Cardholders	29
3.9. Instructional Materials for Child Support Payee Cardholders	31
3.10. Banking Services	31
3.11. Data Transfer	33
3.12. Education and Training	34
3.13. Federal Electronic Fund Transfers	35
3.14. Confidentiality	35
3.15. Conversion	36
3.16. Performance Measures	37
3.17. Compliance	37
3.18. Contract Monitoring Provisions	42
4. FINANCE	44
4.1. Financial Standards	44
4.2. Budget, Staff List and Budget Narrative	47
5. PROPOSAL EVALUATION	48
5.1. Selection	48
5.2. Technical Proposal	48
5.3. Cost Proposal	49
6. PROPOSAL PROCESS	49
6.1. Contact Information – Sole Point of Contact	49
6.2. Procurement Timetable	50
6.3. Letter of Intent	50
6.4. Questions and Answers	51
6.5. Exceptions	51
6.6. RFP Amendment	52
6.7. Proposal Submission	52
6.8. Non-Collusion	53
6.9. Collaborative Proposals	53
6.10. Validity of Proposals	53
6.11. Property of Department	53
6.12. Proposal Withdrawal	53
6.13. Public Disclosure	53
6.14. Non-Commitment	54



6.15. Liability	54
6.16. Request for Additional Information or Materials	55
6.17. Oral Presentations and Discussions	55
6.18. Successful Proposer Notice and Contract Negotiations	55
6.19. Scope of Award and Contract Award Notice	55
6.20. Site Visits	55
6.21. Protest of Intended Award	56
6.22. Contingency	56
6.23. Ethical Requirements	56
7. PROPOSAL OUTLINE AND REQUIREMENTS	56
7.1. Presentation and Identification	56
7.2. Outline and Detail	57
8. MANDATORY BUSINESS SPECIFICATIONS	61
8.1. Contract Terms, Conditions and Liquidated Damages, Forms	61
9. ADDITIONAL INFORMATION	62
9.1. Appendix A – Form P-37 General Provisions and Standard Exhibits	62
9.2. Appendix B – Contract Monitoring Provisions	62
9.3. Appendix C – CLAS Requirements	62
9.4. Appendix D – Price Schedule	62
9.5. Appendix E – Program Staff List	62
9.6. Appendix F – Data Elements for Billing Coupons	62
9.7. Appendix G – SDU Information Technology Provisions Statement of Work	62
9.8. Appendix H – Technical Requirements Checklist	62
9.9. Appendix I - Physical Security Requirements	62
9.10. Appendix J – Required Data Elements for Payment Processing	62
9.11. Appendix K – Statement on Standards for Attestation Engagements (SSAE 16)	62
9.12. Appendix L – Corrective Action/Liquidated Damages Disclosure	62



1. INTRODUCTION

1.1. Purpose and Overview

This Request for Proposals (RFP) is published to solicit proposals for the provision of State Disbursement Unit (SDU) and Electronic Funds Transfer Services (EFT) that include:

- The management and administration of child support billing to payors;
- The management and administration of child support billing to employers;
- The posting of child support payments received;
- The disbursement of Bureau of Child Support Services (BCSS) authorized monies to child support payees;
- The imaging and transmission of all payment information to the Department;
- Associated banking services and check writing; and
- All related services.

The New Hampshire Department of Health and Human Services (Department) anticipates awarding one (1) contract for the services in this RFP.

1.2. Contract Period

The Contract resulting from this RFP is anticipated to be effective December 1, 2021 through December 31, 2031. If a start-up period is needed, the Contract Period may begin as early as September 1, 2021 with 100% service capacity available for January 1, 2022.

The Department may extend contracted services for up to five (5) additional years, contingent upon satisfactory Contractor performance, continued funding, and Governor and Executive Council approval.

2. BACKGROUND

2.1. New Hampshire Department of Health and Human Services, DEHS

The DHHS Division of Economic and Housing Stability (DEHS) seeks positive outcomes for families by focusing on streamlined approaches to services through a lens of the Social Determinants of Health. Its mission is to advance the health, economic and social well-being of individuals, families and communities, envisioning individuals and families being strong, resilient and thriving in their communities. The Bureau of Child Support Services is one of five programs within DEHS.

2.2. Background

Every child living in NH has a legal right to financial support from both parents, even if the parents are divorced, separated or never married. Pursuant to RSA 161:2 XIV and XVI, the NH Department of Health and Human Services, (DHHS), is responsible for establishing, directing and maintaining a program of child support based upon Title IV-D of the Social Security Act as amended. DHHS, through its Bureau of Child



Support Services (BCSS), helps families establish and enforce child support orders - both medical and financial.

An essential component of maintaining a successful child support program includes the operation of a State Disbursement Unit (SDU) that timely and accurately receives, processes, and disburses child support payments. The 1996 enactment of the Personal Responsibility and Work Opportunity Reconciliation Act, Pub. L. 104-193, included a requirement that state Child Support Enforcement agencies operate centralized automated units for collection and disbursement of child support payments.

Highlights of the SDU requirements contained in the law include, but are not limited to, requiring all states: to give employers one and only one location for submitting withheld income; operating the SDU in coordination with the state's CSE automated system; using the SDU to collect and disburse support payments; keeping an accurate identification of payments; promptly disbursing money to custodial parents or other states; furnishing parents with a record of the current status of support payments; using automated procedures, electronic processes, and computer-driven technology to the maximum extent feasible, efficient, and economical; and disbursing to custodial parents all amounts payable within two (2) business days after receiving the money from the employer.

NH implemented its initial SDU in 1999. Beginning in 2002, the Department has utilized contractors to operate an SDU that meets NH's needs and applicable Federal and State regulations. The original Vendor, ACS State & Local Solutions, was purchased in February 2010 by Xerox State & Local Solutions, Inc. This Vendor is currently under contract to provide SDU services. The contract expires December 31, 2021 and is supported with 66% Federal funds and 34% General Funds.

The Bureau of Child Support Services is New Hampshire's designated agency for fulfillment of the US Department of Health and Human Services, Administration for Children and Families (ACF), Title IV-D program. The Federal Office of Child Support Enforcement (OCSE), located within the ACF, provides direction, guidance, and oversight to state IV-D Agencies. OCSE oversees a performance based penalty and incentive system within which states must provide services to child support enforcement (IV-D) cases. Under the incentive system, states can be rewarded for their performance in running an effective IV-D program, or penalized if they fail to perform at acceptable levels. One of the performance measures used to evaluate state performance is cost effectiveness.

The New Hampshire Division of Child Support Services is responsible for the establishment and enforcement of approximately 36,000 child support cases statewide.



2.2.1. Current SDU Information

The SDU uses Department generated data to print and mail bills, identify child support payments received, identify child support disbursements to be issued, perform banking and check-writing functions, as well as electronic funds transfer services. Federal regulations require the SDU to meet standards for data collection, privacy and physical security.

The SDU receives wage assignments from employers and direct payments from child support payors, records and deposits these monies into a specified Department account, and transmits this information to the Department. The information is processed through the Department's child support case management system, the New England Child Support Enforcement System (NECSSES), to determine the appropriate distribution of the child support payments received amongst a child support payor's debts, and to identify the appropriate disbursement of such funds to payee(s). In accordance with Federal regulations, the Department then authorizes the SDU to execute disbursement to the appropriate payee(s). Most payees reside in New Hampshire but others are located in other states or countries.

2.2.1.1. *Transactions Processed Monthly*

Over the last three (3) months, an average of 38,000 child support financial instruments have been received for deposit each month; and an average of 35,000 child support transactions (including disbursements) have been processed at the SDU monthly. Of the 35,000 total disbursements per month, approximately 21,000 were EFT; approximately 2,500 were paper checks; and approximately 11,500 were disbursed via the debit card.

It is anticipated that child support payments received, EFT transactions processed and child support disbursements paid out may increase during the Contract Period.

2.2.1.2. *Imaging and Processing*

The SDU takes and retains an image of payments received, including any documents within the envelope and an image of the envelope itself. The major categories of payments that require imaging and processing (both automated and manual) are listed in Table 1:



Table 1

Payment Type	Approximate Volume of Payments Received
Direct	9.5%
Wage withholding	78.75%
Out-of-state agencies and liens	11.75%

2.2.1.3. Case Types

Direct Payment Cases: the Department produces and provides to the Contractor, in the middle of every month, an electronic file sent by File Transfer Protocol (FTP), from which the Contractor prepares a monthly billing. The Contractor produces and mails a bill containing a statement of each payor's account and payment coupons, for a one-month period, to the payor at least one week prior to the start of the next month. The Contractor provides envelopes or address labels for this billing. The payor receives the entire month's document(s) and then uses a payment coupon to document payments consistent with the ordered frequency.

Court orders create obligations that may require weekly, bi-weekly, semi-monthly, or monthly payments. Currently, in direct payment cases, approximately 7,900 bills are produced monthly, which result in approximately 7,300 transactions per month. Individual bills and coupons are not mailed to payors who are subject to wage withholding. Items received by the Contractor with direct payment transactions include payments and/or correspondence.

Wage Withholding Cases: On a weekly basis, the Department provides to the SDU an employer wage withholding file that contains the information the SDU utilizes for producing Income Withholding Coupons. Every week the Contractor produces and mails Income Withholding Coupons to the employers of payors who are subject to wage withholding. The employer, based on the employer's payroll frequency, returns the Income Withholding Coupons with the payments to the SDU. The date the payment is received at the SDU is the date that is recorded as the receipt date by the Contractor. The Income Withholding Coupons lists the names of all the employees from whose compensation the employer is obligated to withhold child support.



The Contractor uses the Income Withholding Coupons as an input document. The Contractor produces approximately 5,163 copies of Income Withholding Coupons each week, which results in approximately 32,173 transactions per month. Items received by the Contractor with wage withholding transactions include payments and/or correspondence.

Arrearage Only Cases: the Department has an estimated 5,000 "arrearage only" cases. Arrearage cases rarely have changes in scheduled payments. Payments received in arrearage cases are processed in the same manner that direct pay cases and wage withholding cases are processed, as applicable for each case.

Note: Due to the infrequency of cases changes, the Department would consider longer term coupon booklets for these cases, such as three (3) or six (6) month duration.

Out-of-State Cases (OST): Payments are received at the SDU from agencies and other entities in other states. The Contractor processes child support payments received from these agencies.

Each month, there are approximately 4,600 OST payments received, including those made by EFT, and there are approximately 400 financial instruments issued by child support agencies and other entities such as courts, and county agencies. There is no standardized format for these OST payments; each jurisdiction determines their own format.

Items received by the Contractor from out-of-state agencies include payment and/or correspondence.

Lien Cases: Payments are received from banks, insurance companies and other sources that represent payment of liens placed on the payor's assets. The Contractor forwards these payments daily to the Department's designated office.

2.2.1.4. Payment Receiving Sites

The majority of payments are remitted directly to the SDU. Occasionally, payments are received directly in a District Office. Payments received at the district office are forwarded to the SDU in the same manner as payments mailed directly to the SDU.



Payments Received at a District Office: Department staff complete a Payment Receipt, Form 681 (See: Attachment A) for each payment received in a District Office, and logs all payments received on a Record of Daily Receipts, Form A15. The Department staff then forwards the payments, corresponding documentation, and Form A15 to the SDU; the Form A15 summarizes the payments and documentation. The SDU uses the Form 681 as a source document for recording payments received in a district office.

2.2.1.5. *Payment Processing*

For all categories of payment the following activities are an automated process. Daily the selected Vendor must:

- 2.2.1.5.1. Complete imaging for each payment received;
- 2.2.1.5.2. Conduct an analysis and determine whether a payment can be processed, either by an automated process or manually, and acts according to the appropriate Department directions and requirements;
- 2.2.1.5.3. Process unbalanced EFT transactions and cost recovery transactions, and posts actual dollar amounts, and notifies the Department of variances. The Contractor uses a specific code to designate these payments.
- 2.2.1.5.4. Transmit all payment information and provides a written report of such information to the Department;
- 2.2.1.5.5. Deposit all financial instruments, except those that are non-negotiable, to the Department's account;
- 2.2.1.5.6. Forward to the Department an image of all deposited financial instruments and all supporting documentation;
- 2.2.1.5.7. Forward all payments that cannot be deposited because the payment is non-negotiable, to the Department-designated office, with accompanying documentation; and
- 2.2.1.5.8. Forward to the Department all termination of employment information received from an employer, including wage withholding coupons returned with the termination section completed, and any correspondence received.



2.2.1.5.9. The selected Vendor will be expected to process child support payments made via Electronic Funds Transfer/Electronic Data Interchange (EFT/EDI), check, money order, and cash.

2.2.1.6. Disbursing Child Support Payments

Upon receipt of the information described in subsection 2.2.1.5.4 through 2.2.1.5.6., the Department processes the information through its case management system, the New England Child Support Enforcement System (NECSSES), to determine the amount of child support received by the SDU that is payable to the BCSS payee.

The BCSS payee and payor case information is updated accordingly to correctly reflect the amount of support paid by the payor and the amount to be paid to the payee, as well as updating child support and arrears balances.

On a daily basis, the Department transmits payee information, and the child support amount to be paid, as authorization to the SDU to process payment to the payee.

On a daily basis, the SDU receives the information referenced in subsection 2.3.6.3 and issues the payment to the appropriate payee in the form of payment authorized by the payee, such as paper check, direct deposit, and debit card.

2.2.1.7. Electronic Funds Transfer and Electronic Data Interchange (EFT/EDI) Transactions

The current number of EFT/EDI transactions is approximately 22,500 per month. It is expected that the number will increase and the number of transactions handled manually via the SDU will decrease.

The Contractor provides for the collection of child support payments, including a variety of low-cost (to the payor or employer) electronic payment channels, such as money transfer companies, online processing and through mobile devices.

2.3. SDU Audits

Department staff perform financial audits, verifications and research transactions processed by the SDU. In the event an investigation into transactions processed through the SDU is required, DHHS conducts its own investigation.



2.4. Disqualification

The Department, at its sole discretion, may disqualify a Vendor that upon review of the documentation submitted in response to subsection 3.17.6 Audit Requirements and 3.18.5 Statement of Vendor's Financial Condition, is determined to present an unacceptable risk for the successful operation of an SDU.

3. STATEMENT OF WORK

3.1. Scope of Services

3.1.1. Operation Site Requirements

- 3.1.1.1. The selected Vendor must locate its SDU operations within New Hampshire, the exact location of which is subject to Department written approval.

3.1.2. Security

- 3.1.2.1. The selected Vendor must ensure its SDU operation site meets OCSE security requirements, and the requirements specified in Appendix I, Physical Security Requirements.
- 3.1.2.2. The selected Vendor must provide Department-authorized representatives access to its SDU operation site, including for the purpose of conducting forensic investigations and inspections of the physical property on which the SDU contracted services are conducted, at any time. If any SDU services are performed at any location other than the in-state SDU operation site, the Department must be provided the same access to the locations. This must include access to any and all documents, videos and photo/image records. The selected Vendor must cooperate with any Department investigation and make its employees available for interviews, if necessary.

NOTE: Appendix G, SDU Information Technology Provisions Statement of Work, Paragraph 2.3.7, Security Review and Testing, and Paragraph 5.1.2, Topic 2 – System Security and Hosting, addresses the Vendor's Information Technology security provisions for its proposed SDU systems. In responding to paragraph 3.1.2 Security, above, Bidders should describe physical security provisions.

3.1.3. Post Office Box Location

- 3.1.3.1. The selected Vendor must use the following Post Office boxes, as paid for by the Department, located at 955 Goffs Falls Road, Manchester, New Hampshire: PO Box 9501, 9502, 9503 and 9504.



- 3.1.3.2. The Post Office boxes must be used to accept the following paper version documents:
 - 3.1.3.2.1. Employer Payments (PO Box 9501);
 - 3.1.3.2.2. Payor Payments and District Office Receipts (PO Box 9502);
 - 3.1.3.2.3. Out-of-State and International Payments (PO Box 9503); and
 - 3.1.3.2.4. Child Support Payment Enrollment Forms (PO Box 9504).
- 3.1.3.3. In the event of a change in mail volume, or unexpected circumstance, with Department written agreement, the selected Vendor must obtain additional Post Office boxes as necessary.
- 3.1.3.4. Upon termination or expiration of the contract, all Post Office boxes that receive SDU mail must become the property of the Department.
- 3.1.3.5. Post Office Box Content Retrieval
 - 3.1.3.5.1. The selected Vendor must retrieve the contents of Post Office boxes twice daily and deliver such contents to the SDU the same day, Mondays through Saturdays, with the exception of Federally recognized holidays. The selected Vendor must ensure contents retrieved are maintained in a secure and confidential manner, and are immediately, safely and wholly delivered to the SDU operation site for processing. The selected Vendor must ensure that any individuals retrieving and delivering the contents are bonded and insured.

Q1. How will you meet the Operation Site Requirements? Describe, in detail, your operation site for SDU operations.

3.2. Child Support Billing Services

3.2.1. Direct Payment Cases

- 3.2.1.1. The Department will produce and provide monthly billing information, via FTP file transfer, to the selected Vendor each month to enable the selected Vendor to proceed with monthly billing. Appendix F, Required Data Elements for Billing Coupons, displays the billing file format and lists all required data elements and associated character spaces for the monthly bill and coupons.



- 3.2.1.2. For child support payors that choose to receive paper billing, the selected Vendor must utilize Form 684 that includes payment coupons. The selected Vendor must print, produce, fold, stuff, and mail the printed bills and coupons to the payors.
- 3.2.1.3. For child support payors that choose to receive electronic billing, the selected Vendor must utilize an electronic version of monthly bills (Form 684) and associated payment coupons, and electronically transmit these to the payor.
- 3.2.1.4. Coupons must be imprinted or electronically produced with a Magnetic Ink Character Recognition (MICR) line to permit automated processing by an Optical Character Recognition (OCR) device. The coupons must include a space for the payor to indicate that the enclosed payment is a payment for debt other than the payor's regular payment.
- 3.2.1.5. All information appearing on bills and coupons must be individualized.
- 3.2.1.6. Monthly bills, regardless of form, must include New Hampshire's State Seal, which will be provided to the selected Vendor by the Department.
- 3.2.1.7. Monthly bills and payment coupons, regardless of form, are subject to Department acceptance and approval prior to printing or release.
- 3.2.2. **Wage Withholding Cases**
 - 3.2.2.1. The Department will produce and provide weekly billing information, via FTP file transfer, to the selected Vendor each week to enable the selected Vendor to proceed with weekly billing. Appendix F, Required Data Elements for Billing Coupons, displays the billing file format and lists all the required data elements and associated character spaces for the monthly bill and coupons.
 - 3.2.2.2. For employers (of payors that are subject to wage withholding) that choose to receive paper Income Withholding Coupons, the selected Vendor must print the coupons (Income Withholding Coupons), and mail the printed coupons to the employer. Income Withholding Coupons must contain the income withholding information for all employees, of the applicable employer, that are payors in wage withholding cases.



- 3.2.2.3. For employers of payors who are subject to wage withholding that choose to receive electronic billing, the selected Vendor must utilize an electronic version of Income Withholding Coupons (Form 684), and associated payment coupons, and electronically transmit these to the employer. Income Withholding Coupons must contain the income withholding information for all employees subject to wage withholding.
- 3.2.2.4. All information appearing on bills and coupons must be individualized.
- 3.2.2.5. Weekly bills, regardless of form, must include New Hampshire's State Seal.
- 3.2.2.6. Monthly bills and payment coupons, regardless of form, are subject to the Department for acceptance and approval prior to printing or release.
- 3.2.3. **Arrearage Only Cases**
 - 3.2.3.1. The Department will produce and provide arrearage only case billing information, via FTP file transfer, to the selected Vendor to enable the selected Vendor to proceed with monthly billing. See Appendix F, Required Data Elements for Billing Coupons.
 - 3.2.3.2. For child support payors that choose to receive paper billing, the selected Vendor must utilize Form 684 that include payment coupons. The selected Vendor must print, produce, fold, stuff, and mail the bills and coupons to the payor.
 - 3.2.3.3. For child support payors that choose to receive electronic billing, the selected Vendor must utilize an electronic version of monthly bills (Form 684) and associated payment coupons, and electronically transmit these to the payor.
 - 3.2.3.4. Coupons must be imprinted or electronically produced with a MICR line to permit automated processing by an OCR device. The coupons must include a space for the payor to indicate that the enclosed payment is a payment for debt other than the payor's regular payment.
 - 3.2.3.5. All information appearing on bills and coupons must be individualized.
 - 3.2.3.6. Monthly bills, regardless of form, must include New Hampshire's State Seal.



- 3.2.3.7. Monthly bills and payment coupons, regardless of form, are subject to the Department for acceptance and approval prior to printing or release.

3.2.4. **Out-of-State and Lien Cases**

There are no billing requirements for Out-of-State and Lien cases.

3.3. **Processing Payments Received**

3.3.1. Direct Pay Cases

- 3.3.1.1. The selected Vendor must receive direct case payments in paper and electronic forms.
- 3.3.1.2. For payors that choose to remit payment in paper form, the payor returns the applicable payment coupon contained in Form 684 with the payment to the SDU. The selected Vendor must record the date the payment is received at the SDU as the date of receipt.
- 3.3.1.3. For payors that choose to remit payment in electronic form, the payor returns an electronic version of Form 684 with the payment to the SDU. The selected Vendor must record the date the payment is electronically received at the SDU as the date of receipt.
- 3.3.1.4. The selected Vendor must accept other types of payments, including, but not limited to: Automated Clearing House (ACH) payments, debit card, or credit card to complete transactions for the payment of child support.

3.3.2. **Wage Withholding Cases**

- 3.3.2.1. The selected Vendor must receive wage withholding payments, from employers of payors that are subject to wage withholding, in paper and electronic forms.
- 3.3.2.2. For employers that choose to remit payment in paper form, based on the employer's payroll frequency, the employer returns the Income Withholding Coupons with the payment to the SDU. The selected Vendor must record the date the payment is received at the SDU as the date of receipt.
- 3.3.2.3. For employers that choose to remit payment in electronic form, based on the employer's payroll frequency, the employer returns an electronic version of Income Withholding Coupons with the payment to the SDU. The selected Vendor must record the date the payment is electronically received at the SDU as the date of receipt.



- 3.3.2.4. Items received by the selected Vendor with wage withholding transactions include payments and correspondence. The selected Vendor must forward information from correspondence received from employers, such as returned wage withholding coupons that have the termination section completed to indicate termination of employment, electronically to the Department on a daily basis.

3.3.3. **Arrearage Only Cases**

- 3.3.3.1. The selected Vendor must process payments received in arrearage only cases in the same manner as specified in subsection 3.3.1. Direct Pay Cases or subsection 3.3.2. Wage Withholding Cases, as applicable to the case.

3.3.4. **Out-of-State Cases**

- 3.3.4.1. The selected Vendor must process out-of-state child support payments in both paper and electronic forms. There is no standardized format for out-of-state child support payments.
- 3.3.4.2. The selected Vendor must forward information from correspondence received with out-of-state child support payments, if any, to the Department on a daily basis.

3.3.5. **Lien Cases**

- 3.3.5.1. On a daily basis, the selected Vendor must forward payments received in Lien Cases to the Department's Office of Finance for manual processing.

3.3.6. **Payment Processing Requirements for all Case Types**

- 3.3.6.1. The selected Vendor must open, image, and process all mail received in electronic and hard copy form which includes:
 - 3.3.6.1.1. Examining each financial instrument to ensure that it has been made payable to "New Hampshire Department of Health and Human Services" or other payee acceptable to the Department;
 - 3.3.6.1.2. Conducting an analysis and determine whether a payment can be processed, either through an automated or manual process, on the day the payment is received; and



- 3.3.6.1.3. Acting according to the appropriate Department directions and data element requirements by payment/case type specified in Appendix J, Required Data Elements for Payment Processing.

NOTE: For any hard copy mail received by the selected Vendor that has been incorrectly delivered to the SDU, the selected Vendor must return the mail piece to the US Postal Service.

- 3.3.6.2. The selected Vendor must process unbalanced EFT transactions, cost recovery transactions, and post actual dollar amounts for all cases, and must notify the Department of variances. The selected Vendor must use a Department-approved code to designate such payments.
- 3.3.6.3. The selected Vendor must accept and deposit payments denominated in foreign currency. Upon receiving payments denominated in foreign currency, the SDU must immediately initiate conversion to United State dollars. The date that the payment, once converted to United States dollars, is received by the SDU is the date of receipt.
- 3.3.6.4. The selected Vendor must transmit nightly files that contain data as well as images of each day's items.
- 3.3.6.5. The selected Vendor must retain all images for a period of not less than seven (7) years, and will provide the Department with access to any retained image upon request. This provision will survive the life of the resulting contract.
- 3.3.6.6. Direct payments, wage withholding payments, and payments received from out-of-state agencies processed by the selected Vendor must conform to the standard record layout format for daily input to the NECSES system. The selected Vendor must have a Department-approved method for handling exception transactions for direct payments, wage withholding payments, and payments received from out-of-state agencies. All National Automated Clearing House Association (NACHA) approved transactions will be accepted by the Department.



- 3.3.6.7. The selected Vendor must process payments utilizing a batching process in which all financial instruments, documents and receipts are batched separately in accordance with the type of payment which includes: Regular, Wage-Assignment, Out-of-State, and Out-of-State Tax Intercept. The selected Vendor must ensure no batch exceeds one hundred (100) transactions.
- 3.3.6.8. The selected Vendor must make daily deposits to the Department account for all payments that can be deposited. The selected Vendor must electronically forward to the Department an image of all deposited financial instruments and all supporting documentation, including all payment information that can be processed and a written report; the documents and daily report must be forwarded to the Department no later than the day following the processing payments. All original documents related to the processing of payments must be retained by the selected Vendor for sixty (60) days and then destroyed by shredding or incineration.
- 3.3.6.9. The selected Vendor must not process non-negotiable financial instruments including, but not limited to, financial instruments that are: made out to the wrong payee, postdated, unsigned, unreadable, damaged, stale dated (older than six (6) months) or financial instruments that have a legal line that does not match the courtesy line, except as otherwise directed by the Department. The selected Vendor must electronically forward all payments that cannot be deposited because the payment is non-negotiable, with accompanying documentation to the Department on a daily basis.
- 3.3.6.10. The selected Vendor must conduct research on all child support payments received in the SDU that have incomplete or invalid payment information. Research is an "in-stream" activity occurring on the day the payment is received in the SDU. The Research function consists of examining validation data elements to determine the appropriate identifying information for the payment to ensure that it is posted to the correct account.
- 3.3.6.11. The Department will provide the following validation data elements, for each child support case:
 - 3.3.6.11.1. Payor name;
 - 3.3.6.11.2. Payor case identification number;



- 3.3.6.11.3. Payor member ID number;
- 3.3.6.11.4. Payor Social Security Number;
- 3.3.6.11.5. Payee name;
- 3.3.6.11.6. Current employer name, town and telephone number, if applicable;
- 3.3.6.11.7. Wage assignment in effect, if applicable; and
- 3.3.6.11.8. Current weekly support amount if any wage assignment in effect.
- 3.3.6.12. The Department will load validation data into the selected Vendor's cross-reference database to enable the selected Vendor's SDU staff to access the data for research purposes.
- 3.3.6.13. The selected Vendor's research efforts must result in one of two outcomes:
 - 3.3.6.13.1. Successful identification of a payment, in which case the correct payor/case ID is established, recorded, and the payment information will be included in that evening's transmission to the Department, and the corresponding instrument is deposited in the bank; or,
 - 3.3.6.13.2. No identification of a payment, in which case a generic ID (AAA00000) is assigned to the payment, recorded, and the payment information will be included in that evening's transmission to the Department, and the corresponding financial instrument will be deposited in the bank.
- 3.3.6.14. The selected Vendor must provide a separate monthly report that includes daily and weekly itemizations for Direct Payment, Wage Withholding, and Out-of-State (including Out-of-State Tax Intercept) payments received and processed, and the total number of processing services performed each day within those categories for the month.



- 3.3.6.15. The selected Vendor will be responsible for screening and tracking Non-Sufficient Fund (NSF) checks, once provided electronic notice from the Department of all payors for whom personal checks may no longer be accepted. After this notice is received, the selected Vendor must indemnify and hold harmless the Department for any checks from the identified payors not honored by the bank. The amount of the indemnity includes, but is not limited to, the amount of the check and all fees and associated costs. The Department will provide written notice to the selected Vendor that specifies the amount, date and check number, and payor name, routing transit number, bank account number and name(s) on the account.

3.3.7. Posting Errors

- 3.3.7.1. The selected Vendor will be responsible for correctly analyzing, classifying, recording and posting all payments. Incorrectly recorded or posted payments can result in incorrect distribution of payments. The selected Vendor will be held liable for these errors, pursuant to the process described in subparagraph 4.1.3.4.

Q2. How will you meet the requirements stated in subsection 3.3. Processing Payments Received? Include your process for completing payment processing requirements and the delivery method that will be used to forward the imaged documentation and daily reports to the Department.

3.4. Disbursing Child Support Payments

3.4.1. BCSS Authorization

- 3.4.1.1. Upon receipt of the information described in subsection 3.3.6 Payment Processing Requirements for all Case Types, the Department will process the information through NECSES on a daily basis, to determine the amount of child support received by the SDU that is payable to the child support payee. The Department will then electronically transmit this information to the selected Vendor as authorization to generate payment to the child support payee.

3.4.2. Disbursing Authorized Payments

- 3.4.2.1. The selected Vendor will electronically receive payment information from the Department and initiate and process the appropriate payment to the appropriate payee within twenty-four (24) hours of receiving the information.



- 3.4.2.2. The selected Vendor will provide payees with a variety of methods and forms with which to receive payments, including but not limited to direct deposit or a debit card. NOTE: Paper checks are used in special circumstances only, subject to the Department approval.

Q3. How will you meet the requirements stated in subsection 3.4? Include the process you will use to disburse Child Support Payments. Identify the methods and forms of payment that will be available to payees, and specify any associated costs to the payees by method and form of payment.

3.5. Electronic Funds Transfer and Electronic Data Interchange Services (EFT/EDI)

- 3.5.1.1. The selected Vendor must arrange for and provide, accept, and process EFT/EDI transactions for the collection and disbursement of child support payments. The selected Vendor must offer payors and/or employers low-cost electronic payment channels which may include, but are not limited to:

3.5.1.2. Debit cards.

3.5.1.3. On-line processing.

3.5.1.4. Mobile applications via mobile devices.

3.5.2. Electronic Payments Provisions for Employers

- 3.5.2.1. The selected Vendor must provide a method(s) for employers to remit child support payments electronically. The method(s) used must permit the employer to convert the information to either CCD+ or CTX/820 format. The method(s) used will be the means for the employer to prepare the EFT/EDI file to be sent to the bank in a format that conforms to the NACHA standard.

3.5.3. Cardholder Provisions for Child Support Payees

- 3.5.3.1. The selected Vendor must make debit cards available to child support payees for the disbursement of child support and for account balance information. For those individuals who choose to participate in this method of EFT, the selected Vendor must provide the initial debit card to the cardholder at no cost to the Department or the cardholder.
- 3.5.3.2. The selected Vendor must provide a debit card program that is an industry standard application, primarily using existing commercial networks and retailers' Point of Service (POS) devices.



- 3.5.3.2.1. The debit card must be a branded VISA or MasterCard, must operate via the VISA or MasterCard network and must be accepted by any participating merchant.
- 3.5.3.2.2. The debit card must require a Personal Account Number and/or signature for activation and purchases.
- 3.5.3.2.3. The selected Vendor must provide a magnetic or chip debit card that: is fully compliant with all federal laws and regulations; meets industry standards, including current Payment Card Industry (PCI) standards, for quality; contains security features to activate the card and prevent counterfeiting.
- 3.5.3.3. The selected Vendor will be responsible for production and issuance of the initial and replacement debit cards. The Department will have final approval of the design, content, and process of distribution of the card mailer.
- 3.5.3.4. The selected Vendor will be responsible for the appropriate handling and resolution of debit cards that:
 - 3.5.3.4.1. Are returned to the selected Vendor by the US Post Office, and notifying the Department of return.
 - 3.5.3.4.2. Are returned to the selected Vendor by the US Post Office with forwarding address information provided by the US Post Office, and notifying the Department of return.
 - 3.5.3.4.3. Are expired. The selected Vendor must specify the expiration timeframe of cards from the issue date and reissue cards to replace the expired cards. The selected Vendor must provide to active cardholders detailed procedures for the reissuance of cards due to expire, including at minimum: the timeframe for reissuance of the card; the procedure for the cardholder to activate the new card; the new account number and account activity balance; and instructions on activating the Personal Identification Number.
 - 3.5.3.4.4. Are unpinned by the cardholder and have funds deposited on the card. The selected Vendor must:



- 3.5.3.4.4.1. Provide a weekly report to the Department of cards with funds deposited and not pinned and/or activated by the cardholder. The report must include the name, address, telephone number, date of card issuance and the first date of funds deposited to the card.
- 3.5.3.4.4.2. Conduct outreach to cardholders. The outreach process and procedure will be subject to Department approval.
- 3.5.3.4.4.3. Provide a detailed procedure for the Department to request retrieval of funds from the card. The procedure must include but not be limited to: the timeframe for the retrieval of funds; the method of payment of the funds; the notification to the Department of retrieval of the funds; and the method of forwarding the funds to the Department.
- 3.5.3.4.5. Are lost, stolen or require replacement other than for the reason of being expired. The selected Vendor must provide to cardholders detailed terms and conditions for the replacement of debit cards that include at minimum:
 - 3.5.3.4.5.1. Defining what constitutes a replacement card.
 - 3.5.3.4.5.2. The procedure for requesting a replacement card.
 - 3.5.3.4.5.3. The timeframe within which a replacement card will be issued.
 - 3.5.3.4.5.4. The procedures and conditions for expediting a replacement card.
- 3.5.3.5. The selected Vendor must maintain the confidentiality of any and all cardholder information and cardholder account information. The selected Vendor must ensure that cardholder information and cardholder account information is protected and kept confidential.



- 3.5.3.6. The selected Vendor must not sell or share cardholder information and cardholder account information with any other entity not associated with this contract or for any purpose other than the execution of the contract, unless required by federal or state law.
- 3.5.3.7. The selected Vendor must not use cardholder information or cardholder account information to solicit business.
- 3.5.3.8. The selected Vendor must provide written notification to the Department of any changes affecting cardholders ninety (90) calendar days prior to the effective date of any change. Changes include but are not limited to: changes in debit card policies or procedures; program rules; or adjustments to the cardholder's account balance. All changes are subject to the Department's approval.
- 3.5.3.9. The selected Vendor must provide written notification to cardholders of any changes thirty (30) calendar days prior to the effective date of any change. The content of any and all notifications to the cardholders must be approved by the Department.

Q4. Describe in detail any and all conditions and terms the Bidder proposes to impose on cardholders. Include at minimum:

- *The replacement of debit cards.*
- *What constitutes a replacement card.*
- *Procedure for requesting a replacement card.*
- *Timeframe within which the debit card will be replaced*
- *Procedure and conditions for expediting a replacement card issuance.*
- *Limitations on cardholder use of a debit card (such as number of transactions by type permitted per day by cardholder, minimum and maximum withdrawal amounts by site type, and maximum amount available for withdrawal daily).*
- *Fees or surcharges that the Bidders proposes to impose on cardholders by transaction type.*
- *Free transactions and services that will be provided to the cardholder and at what quantity.*

3.5.4. Automated Teller Machine (ATM) Access for Child Support Payee Cardholder



- 3.5.4.1. The selected Vendor must provide debit card access through an operating ATM network allowing for national and international ATM access with withdrawal of cash through a normal ATM transaction.

Q5. Describe in detail the Vendor's ATM network. Include the total number of network ATM locations and indicate where cardholders can use their cards without incurring ATM surcharge or other type of surcharge. Provide the total number of surcharge-free ATM locations. Describe in detail how the Vendor will provide ATM access to cardholders who reside outside of New Hampshire and outside of the United States.

3.5.5. Point of Service (POS) Access for Child Support Payees

- 3.5.5.1. The selected Vendor must ensure the child support payee cardholder is able to use the debit card to purchase goods and services anywhere the brand (Visa/MasterCard) is accepted. The cardholder must be able to use the debit card in a variety of ways including but not limited to:

- 3.5.5.1.1. Internet.

- 3.5.5.1.2. Mail order.

- 3.5.5.1.3. Telephone order purchases.

- 3.5.5.2. The selected Vendor must ensure the operating network can query the cardholder's available balance at the time of any PIN-based POS transaction and disallow those transactions that would exceed the cardholder's balance.

- 3.5.5.3. The selected Vendor must ensure the cardholder will be able to receive cash back with a POS transaction based on either the store limit or the negotiated cash back withdrawal limit.

Q6. Describe in detail how cards issued to cardholders will be accepted by any participating merchant or service provider network using a POS device. Describe in detail how the Vendor will process and document PIN-based and signature-based purchases and other transactions.

3.5.6. Bank Teller Access for Child Support Payees

- 3.5.6.1. The selected Vendor must provide child support payee cardholders with access to cash withdrawals, utilizing debit cards, through the use of bank tellers.

Q7. Describe in detail how the debit card will be accepted by any participating bank location for bank teller cash withdrawal access, the total number of bank locations that will accept use of the debit card, and the process for a cash withdrawal, through the use of a bank teller, to which child support payee cardholders would be subject.



3.5.7. Payment Acceptance

- 3.5.7.1. Regardless of whether payors or employers choose to receive coupons in paper form, the selected Vendor must accept payments made in either paper or electronic form.

3.5.8. EFT/EDI Transaction Processing for Child Support Payee Cardholders

- 3.5.8.1. The selected Vendor must accept transactions from an authorized transaction merchant.
- 3.5.8.2. The selected Vendor must ensure each transaction is properly posted based upon the availability of funds. The selected Vendor must ensure that transactions are denied if any of the following conditions are met:
- 3.5.8.2.1. The number of consecutive failed PIN tries have been exceeded.
- 3.5.8.2.2. There are insufficient funds to process the transaction.
- 3.5.8.3. The selected Vendor must appropriately authorize or deny EFT and EDI transactions regarding a cardholder's account, including denying any that may be disallowed or cause the cardholder to exceed the amount available in their account. The selected Vendor must send response messages to the merchant that authorize or reject the transaction.
- 3.5.8.4. The selected Vendor must log authorized and denied transactions for subsequent settlement and reconciliation processing, and for inclusion in transaction reporting and viewing through transaction history.

Q8. Describe in detail how the Vendor will meet the requirements of subsection 3.5.8 EFT/EDI Transaction Processing for Child Support Payee Cardholders. Include the turnaround time for processing transactions; the Vendor's processing accuracy rates; and samples of the messages typically issued by the Vendor to merchants when transactions are rejected.

3.6. Self-Service Web Portal

3.6.1. Accessibility

- 3.6.1.1. The selected Vendor must provide child support payors, child support payees, and employers with a secure web-based site that is accessible twenty-four (24) hours per day, seven (7) days per week.



3.6.2. Services Available

- 3.6.2.1. The selected Vendor must ensure the Self-Service Web Portal will provide an array of services and information to users based on user type, including but not limited to:
 - 3.6.2.1.1. Allowing the electronic payment of direct child support and wage withholding payments by child support payors and employers.
 - 3.6.2.1.2. Viewing of child support and wage withholding bills.
 - 3.6.2.1.3. Confirming payment receipts.
 - 3.6.2.1.4. Viewing on-line statements of detailed financial transactions posted to their account.
 - 3.6.2.1.5. Viewing detailed deposit information.
 - 3.6.2.1.6. Viewing additional notification and information regarding use of cards for payees.
 - 3.6.2.1.7. Viewing frequently Asked Questions (FAQs) regarding the services delivered by the SDU, Help Desk contact information for the SDU.
 - 3.6.2.1.8. Accessing customer Services support and assistance for users of the Self-Service Portal.
 - 3.6.2.1.9. Accessing hyperlinks to the New Hampshire Bureau of Child Support website.
- 3.6.2.2. The selected Vendor must provide a user-friendly and simple on-line registration process to access the Self-Service Portal.
- 3.6.2.3. The Department will have final approval of the design and content of the web portal.
- 3.6.2.4. The selected Vendor must, at Department discretion, provide access to all of the information described in subsection 3.6.2.1, through a smartphone application.

Q9. Describe in detail the method and process for individuals to access and use the Self Service Web Portal, as described in subsection 3.6. Explain how individuals will navigate within the portal. Include any other services the Vendor proposes to make available to payors, payees, and employers through the Self Service Web Portal.

Q10. Describe in detail how the Vendor will meet the following requirements:

- *The method of notifying the Department of changes in policy or procedures affecting individuals using the Self Service Web Portal.*



- *The method in which individuals will be notified of changes in policy and procedures affecting them.*
- *The method in which child support payors and payees will be notified of adjustments to their account balances when adjustments are required and performed by the Vendor.*
- *The method of receiving and resolving complaints and disputes, and the timeframe for the resolution.*

3.7. Automated Response Unit (ARU) for Child Support Payees

3.7.1. ARU Accessibility

- 3.7.1.1. The selected Vendor must provide child support payee cardholders with access to an Automated Response Unit (ARU) twenty-four (24) hours per day, seven (7) days per week.
- 3.7.1.2. The ARU must contain the functionality for cardholders to exit ARU and be transferred directly to a customer services representative in the Cardholder Help Desk at any time.
- 3.7.1.3. The selected Vendor must have policies and standards in place for the ARU that addresses the number of rings prior to answer, and the average time a cardholder remains on hold, to ensure child support payee timely access to ARU services. The policies and standards are subject to Department approval.
- 3.7.1.4. The selected Vendor must provide the Department with monthly reports of ARU activity, including but not limited to the number of calls; the number of calls dropped; and the number of callers that opted to access Customer Service for further assistance.

3.7.2. Card Activation, PIN Setting and Changing

- 3.7.2.1. The selected Vendor must ensure the ARU enables cardholders to activate their debit card. The selected Vendor must provide cardholders with secure ARU PIN select procedures and instructions to activate their debit card through the ARU.
- 3.7.2.2. The selected Vendor must ensure the ARU enables cardholders to change the PIN for their debit card. The selected Vendor must provide cardholders with secure ARU PIN change procedures and instructions to change the PIN for their debit card through the ARU.



3.7.3. Other ARU Transactions

- 3.7.3.1. The selected Vendor must ensure the ARU enables cardholders to report a lost, stolen or damaged debit card. The selected Vendor must provide cardholders with a secure ARU process and detailed instructions to complete such reporting through the ARU.
- 3.7.3.2. The selected Vendor must ensure the ARU enables cardholders to obtain the cardholder's real time account balance information. The selected Vendor must provide real-time account balance information to cardholders, and must state what is defined as real-time account balance.
- 3.7.3.3. The selected Vendor must ensure the ARU enables cardholders to obtain the transaction history for their account. The selected Vendor must provide the cardholder with the transaction history and clearly state the maximum number of transactions included in the history.
- 3.7.3.4. The selected Vendor must clearly detail additional transaction information available to the cardholder and the method of obtaining that information.
- 3.7.3.5. The selected Vendor must ensure the ARU enables cardholders to receive through the ARU information about:
 - 3.7.3.5.1. The methods to report unauthorized use of the debit card, one of which must include reporting through the ARU.
 - 3.7.3.5.2. How potential fraudulent transactions are identified and the procedures for handling and reporting any potential fraudulent transactions.
- 3.7.3.6. The selected Vendor must have a reporting process and capabilities, including how the selected Vendor provides reports to the Department to the extent permissible under 12 CFR 205 Regulation E and industry guidelines.
- 3.7.3.7. The selected Vendor must ensure the ARU contains the functionality for cardholders to opt out to a customer services representative at any time.

Q11. Describe in detail how you will fulfill the requirements of the ARU, as described in subsection 3.7 Automated Response Unit (ARU) for Child Support Payees. Identify any other services you will make available to payors and payees through the ARU.

3.8. Customer Services for Child Support Payee Cardholders



3.8.1. **Cardholder Help Desk Operation**

3.8.1.1. The selected Vendor must provide child support payee cardholders with telephone access to a Cardholder Help Desk twenty-four (24) hours per day, seven (7) days per week. The selected Vendor must ensure the Help Desk services provides current debit card account; deposit; withdrawal; and transaction history information via a toll-free, number that is available in-state, out-of-state, and internationally.

3.8.1.1.1. The selected Vendor must ensure customer service representatives are available to resolve issues that cannot be resolved through the Automated Response Unit (ARU).

3.8.1.1.2. The selected Vendor must ensure customer service representative capacity is able to meet the demand for cardholder calls referred to the Cardholder Help Desk.

3.8.1.2. The selected Vendor must ensure the Cardholder Help Desk enables cardholders to process the same transactions, through telephone access to the Cardholder Help Desk, described in paragraph 3.7.2 Card Activation, PIN Setting and Changing as well as paragraph 3.7.3 Other ARU Transactions.

3.8.2. **Cardholder Help Desk Accessibility**

3.8.2.1. Cardholder Help Desk services must be provided in English and Spanish. The individuals providing customer service must be proficient in written and spoken English and have a clear comprehension of the English language. Any individual the selected Vendor designates for providing customer services in Spanish must also be proficient in written and spoken Spanish and have a clear comprehension of the Spanish language, in addition to the English language.

3.8.2.2. The selected Vendor must provide the services described in subsections 3.7 Automated Response Unit (ARU) for Child Support Payee Cardholders and 3.8 Customer Services for Child Support Payees to payees requiring use of Teletypewriter (TTY) services.

3.8.3. **Additional Cardholder Help Desk Requirements**

3.8.3.1. The selected Vendor must have procedures in place to ensure and verify the identity of the cardholder using the Cardholder Help Desk or the Self-Service Web Portal.



- 3.8.3.2. The selected Vendor must have a monitoring program in place to ensure quality customer services are delivered, through the ARU and Cardholder Help Desk.
- 3.8.3.3. The selected Vendor must ensure customer services are available via teletypewriter (TTY) and communications relay capability as described in the Americans with Disabilities Act.
- 3.8.3.4. The selected Vendor must ensure that phone calls are answered within six (6) rings with limited drop calls and an average hold time of three (3) minutes.

Q12. How will you ensure and verify the identity of the cardholder using the Cardholder Help Desk and Self Service Web Portal?

Q13. Provide your proposed plan to meet or exceed the requirements in 3.8.3.

3.9. Instructional Materials for Child Support Payee Cardholders

- 3.9.1. The selected Vendor must provide instructional materials to child support payee cardholders that are written in English and Spanish at a reading level no higher than sixth (6th) grade.
- 3.9.2. The selected Vendor must include training materials in the card issuance packet to ensure the cardholder understands how to activate the account; cardholder rights and responsibilities; how to use the card; identification of any and all associated fees; and where to call for questions and reporting issues.
- 3.9.3. The selected Vendor must obtain Department approval of all instructional materials that will be sent to the cardholder at the time of card issuance.

Q14. Describe all web pages, instructional materials, marketing materials, statements, and any other forms related to the debit card process the Vendor proposes to provide cardholders. Provide samples.

3.10. Banking Services

3.10.1. Minimum Requirements

- 3.10.1.1. The selected Vendor must provide, either directly or indirectly, banking services to support and facilitate SDU service delivery which must include, but are not limited to:
 - 3.10.1.1.1. A dedicated SDU-BCSS bank account, which must be held in a NH bank, for SDU transactions to be processed through. The bank account will be the depository for BCSS payments. The selected Vendor must deposit all payments on the date of receipt. Daily deposited funds that are available to BCSS must be transferred via



ACH on a daily basis. If any deposited funds are not available on the day of initial deposit, an earnings credit must be given on any balance left on deposit and it will be based on the average collection balance. The earnings credit must be used against SDU charges with the balance of the charges to be billed monthly.

- 3.10.1.1.2. Each child support payment received must be endorsed with a stamp stating the following, unless otherwise designed by BCSS:

FOR DEPOSIT ONLY
Department of Health and Human Services
BCSS
(with the bank account number)

- 3.10.1.2. The selected Vendor must record on the back of each payment the batch number, sequence number and the date of deposit. The selected Vendor must ensure the front of the check includes a Magnetic Ink Character Recognition (MICR) line indicating the check number; routing number; and account number. The selected Vendor must ensure account maintenance includes, but is not limited to:

- 3.10.1.2.1. Acceptance of deposits, endorsement and imaging of all checks and other financial instruments deposited into the dedicated SDU-BCSS bank account.
- 3.10.1.2.2. Encoding of checks with check amount.
- 3.10.1.2.3. Service dishonored and returned checks presented for deposit into the dedicated SDU-BCSS bank account.
- 3.10.1.2.4. Maintenance and reconciliation of the dedicated SDU-BCSS bank account.
- 3.10.1.2.5. Provision of EFT services, CD-ROM, or other electronic medium for the dedicated SDU-BCSS bank account.
- 3.10.1.2.6. Provision of EDI translation.
- 3.10.1.2.7. Provision of copies of paid checks, monthly statements, on-line access to accounts, and check safekeeping.



3.10.1.2.8. Provision of all banking facilities and services normally delivered to checking account customers, including, but not limited to: deposit slips and other instruments pertaining to the account and usual and generally accepted banking services associated with this type of account.

3.10.1.3. The selected Vendor must make a copy of the deposit slip available to the Department's designated staff and/or office for each day's activity no later than the following day of deposit.

3.10.1.4. The selected Vendor must retain a copy of all payments deposited for a period of not less than seven (7) years. The copies will be retained on an appropriate medium. The selected Vendor must provide the Department with access to any retained image upon request. This provision will survive the life of the Contract

3.10.1.5. The selected Vendor must provide check writing services that ensure the timely printing of child support checks from the SDU-BCSS bank account. Past utilization indicates an average of 2,500 checks are printed on a monthly basis.

Q15. Provide your proposed plan to meet the required banking services described in subsection 3.10 Banking Services. Identify the banking provider and specify any associated banking fees by transaction type and any limitations.

3.11. Data Transfer

3.11.1. From Contractor to BCSS

3.11.1.1. The selected Vendor must transmit keyed information and the EFT receipt files on the date of processing to the Department. The selected Vendor must ensure the BCSS receives both the transmission for keyed information and the EFT receipt file no later than 6:00 PM (EST).

3.11.1.2. The selected Vendor must transmit files to the Department through a secure and encrypted method.

3.11.2. From BCSS to Contractor

3.11.2.1. BCSS will transmit an FTP file to the selected Vendor, each month for child support payors and each week for employers that contains the billing information for child support payors and employers. Files may be transmitted more often as requested by the selected Vendor.



- 3.11.2.2. BCSS will transmit reconciled payment authorization information to the selected Vendor in order that the Vendor can generate child support payments to the appropriate payees.

NOTE: Appendix G, SDU Information Technology Provisions Statement of Work, Paragraph 5.1.1, Topic 1 – Data Exchange, addresses the mechanisms and tools included in the proposed SDU system to enable the specified data sharing between the Vendor and BCSS for the transmission of customer and EBT data within the SDU to financial institutions and BCSS. In responding to section 3.11, Vendors should address those elements of Data Transfer not otherwise addressed in Appendix G.

3.11.3. Criminal Background, Drug Screening and Disclosures

- 3.11.3.1. Prior to a prospective employee's first day of work, the selected Vendor must conduct and receive a comprehensive drug screening and background check, including a criminal records check, on any employee who shall perform duties under this Contract. A copy of said background check shall be provided to BCSS upon request. This background check process applies to temporary employees each time they start or re-start work with the selected Vendor. The background check shall include at a minimum, identity verification, including Social Security Number trace, and felony and misdemeanor records from county of current residence.
- 3.11.3.2. All selected Vendor employees, permanent and temporary, shall sign a disclosure form provided by BCSS which discloses any relationship of their own, or of a member of their immediate family, to the process of receiving or paying child support. These disclosure forms shall immediately be shared with BCSS. The Contractor's employees shall be strictly prohibited from accessing the system to check the status of cases to which they have a personal relationship. No employee shall process transactions or documents related to a child support case to which they have a personal relationship.

3.12. Education and Training

- 3.12.1. The selected Vendor must have a plan for providing continuing education, training and technical assistance for BCSS staff, as requested and approved by BCSS, regarding SDU contracted services. The dates, times and locations of trainings must be agreeable to both the selected Vendor and the Department.

Q16. Provide your proposed education and training plan that will minimize impact on day-to-day business operations.



3.13. Federal Electronic Fund Transfers

3.13.1. The selected Vendor must provide BCSS with reporting to the extent permissible under 12 CFR 205 Regulation E and industry guidelines.

Q17. Describe the reporting processes and capabilities that the Vendor proposes to provide to BCSS, including referencing the applicable industry guidelines.

3.14. Confidentiality

3.14.1. The selected Vendor must utilize detailed policies and procedures that ensure confidentiality for SDU contracted services is maintained.

3.14.2. The selected Vendor must ensure all policies and procedures are consistent with the requirements of state and federal privacy laws and NH RSA 359-C relating to confidentiality of personal identifiable information, financial information, breach notification.

3.14.3. All policies and procedures are subject to BCSS approval.

3.14.4. The Department reserves the right to terminate the resulting contract if confidentiality is breached.

3.14.5. **BCSS Disaster Recovery**

3.14.5.1. Upon notice of or becoming aware of the Department's declaration of a Department information technology related disaster, the selected Vendor must immediately communicate with the BCSS Business Recovery Services Contractor. The selected Vendor must perform all its contractual duties in cooperation with the Business Recovery Services Contractor, and at the direction of the Department of Information Technology (DoIT), until such time as DoIT's mainframe is fully operational. Information regarding the Point-of-Contact for the Business Recovery Services Contractor will be provided to the selected Vendor by BCSS upon contract execution.

NOTE: Appendix G, SDU Information Technology Provisions Statement of Work, Paragraph 5.1.3, Backup and Recovery, addresses the Contractor's disaster recovery provisions for its proposed SDU systems.

3.14.6. **Statements on Standards for Attestation Engagements (SSAE 16)**

3.14.6.1. The selected Vendor must comply with the requirements regarding SSAE 16 contained in Appendix K, Statement on Standards for Attestation Engagements (SSAE 16).



3.15. Conversion

3.15.1. Vendor Transition

NOTE: Appendix G, SDU Information Technology Provisions Statement of Work, subsection 4.5, Contingency Plan / Disaster Recovery Plan, and subsection 5.2.1, Topic 5 – Transition and Implementation Services, apply to Information Technology related transition and implementation requirements between BCSS and the Vendor. The following provisions are focused primarily on the transition as it pertains to the potential impact on BCSS child support stakeholders.

- 3.15.1.1. The selected Vendor must work with BCSS, and any other organizations designated by BCSS, to ensure an orderly Transition Phase to ensure continuity of services required by BCSS. The selected Vendor must work in an organized manner with BCSS and the current SDU contractor to ensure a smooth and timely transition of services.
- 3.15.1.2. During the Transition Phase, the selected Vendor must support a formalized system to report problems and an effective capability to identify problems, identify personnel responsible for problem resolution, estimate timeframes for resolution, monitor status of all problems, invoke escalation procedures, and maintain a formal record of the final outcome.
- 3.15.1.3. The Transition Plan must detail steps and procedures that will assist debit cardholders with a smooth transition ensuring no disruption to redemption of benefits by cardholders.
- 3.15.1.4. The selected Vendor must describe the anticipated methodology for transitioning the debit card database between the existing SDU system and the selected Vendor's SDU system. The selected Vendor must ensure no disruption to cardholder benefit access and services throughout the conversion process.

3.15.2. Preparation and Testing

- 3.15.2.1. The selected Vendor must prepare, design, implement, and test all requirements as specified in Sections 3.15 of this RFP.

NOTE: Appendix G, SDU Information Technology Provisions Statement of Work, Section 2, Testing and Acceptance, addresses testing requirements, planning and preparation, scheduling, user-acceptance testing, and security review and training. In responding to 3.15.2.1, Bidders should describe those elements of preparation and testing that are not specific to the requirements described in Appendix G, Section 2.



3.16. Performance Measures

- 3.16.1. The Department seeks to actively and regularly collaborate with providers to enhance contract management, improve results, and adjust program delivery and policy based on successful outcomes.
- 3.16.2. The Department may collect other key data and metrics from Contractor(s), including client-level demographic, performance, and service data.
- 3.16.3. The Department may identify expectations for active and regular collaboration, including key performance measures, in the resulting contract. Where applicable, Contractor(s) must collect and share data with the Department in a format specified by the Department.

3.17. Compliance

- 3.17.1. Contractor(s) must be in compliance with applicable federal and state laws, rules and regulations, and applicable policies and procedures adopted by the Department currently in effect, and as they may be adopted or amended during the contract period.
- 3.17.2. The selected Vendor must meet all information security and privacy requirements as set by the Department.
- 3.17.3. The selected Vendor must maintain the following records during the resulting contract term where appropriate and as prescribed by the Department:
 - 3.17.3.1. Books, records, documents and other electronic or physical data evidencing and reflecting all costs and other expenses incurred by the Contractor in the performance of the Contract, and all income received or collected by the Contractor.
 - 3.17.3.2. All records must be maintained in accordance with accounting procedures and practices, which sufficiently and properly reflect all such costs and expenses, and which are acceptable to the Department, and to include, without limitation, all ledgers, books, records, and original evidence of costs such as purchase requisitions and orders, vouchers, requisitions for materials, inventories, valuations of in-kind contributions, labor time cards, payrolls, and other records requested or required by the Department.
 - 3.17.3.3. During the term of this Contract and the period for retention hereunder, the Department, the United States Department of Health and Human Services, and any of their designated representatives shall have access to all reports and records maintained pursuant to the Contract for purposes of audit, examination, excerpts and transcripts. Upon the purchase by



the Department of the maximum number of units provided for in the Contract and upon payment of the price limitation hereunder, the Contract and all the obligations of the parties hereunder (except such obligations as, by the terms of the Contract are to be performed after the end of the term of this Contract and/or survive the termination of the Contract) shall terminate, provided however, that if, upon review of the Final Expenditure Report the Department shall disallow any expenses claimed by the Contractor as costs hereunder the Department shall retain the right, at its discretion, to deduct the amount of such expenses as are disallowed or to recover such sums from the Contractor.

3.17.4. Credits and Copyright Ownership

- 3.17.4.1. All documents, notices, press releases, research reports and other materials prepared during or resulting from the performance of the services of the Contract shall include the following statement, "The preparation of this (report, document etc.) was financed under a Contract with the State of New Hampshire, Department of Health and Human Services, with funds provided in part by the State of New Hampshire and/or such other funding sources as were available or required, e.g., the United States Department of *Health and Human Services*."
- 3.17.4.2. All written, video and audio materials produced or purchased under the contract shall have prior approval from the Department before printing, production, distribution or use.
- 3.17.4.3. The Department will retain copyright ownership for any and all original materials produced, including, but not limited to:
 - 3.17.4.3.1. Brochures.
 - 3.17.4.3.2. Resource directories.
 - 3.17.4.3.3. Protocols.
 - 3.17.4.3.4. Guidelines.
 - 3.17.4.3.5. Posters.
 - 3.17.4.3.6. Reports.
- 3.17.4.4. The selected Contractor(s) shall not reproduce any materials produced under the contract without prior written approval from the Department.



3.17.5. Culturally and Linguistically Appropriate Services

- 3.17.5.1. The Department is committed to reducing health disparities in New Hampshire and recognizes that culture and language can have a considerable impact on how individuals access and respond to health and human services. Culturally and linguistically diverse populations experience barriers in their efforts to access services. As a result, Department is strongly committed to providing culturally and linguistically competent programs and services for its clients, and as a means of ensuring access to quality care for all. As part of that commitment, Department continuously strives to improve existing programs and services, and to bring them in line with current best practices.
- 3.17.5.2. The Department requires all Contractors and sub-recipients to provide culturally and linguistically appropriate programs and services in compliance with all applicable federal civil rights laws, which may include: Title VI of the Civil Rights Act of 1964, the Americans with Disabilities Act of 1990, the Age Discrimination Act of 1975, and the Rehabilitation Act of 1973. Collectively, these laws prohibit discrimination on the grounds of race, color, national origin, disability, age, sex, and religion.
- 3.17.5.3. There are numerous resources available to help recipients increase their ability to meet the needs of culturally, racially and linguistically diverse clients. Some of the main information sources are listed in the Bidder's Reference Guide for Completing CLAS Section of the RFP, and, in the Vendor/RFP section of the Department's website.
- 3.17.5.4. A key Title VI guidance is the National Standards for Culturally and Linguistically Appropriate Services in Health Care (CLAS Standards), developed by the U.S. Department of Health and Human Services in 2000. The CLAS Standards provide specific steps that organizations may take to make their services more culturally and linguistically appropriate. The enhanced CLAS standards, released in 2013, promote effective communication not only with persons with Limited English Proficiency, but also with persons who have other communication needs. The enhanced Standards provide a framework for organizations to best serve the nation's increasingly diverse communities.



- 3.17.5.5. Contractors are expected to consider the need for language services for individuals with Limited English Proficiency as well as other communication needs, served or likely to be encountered in the eligible service population, both in developing their budgets and in conducting their programs and activities.
- 3.17.5.6. Successful Contractors will be:
 - 3.17.5.6.1. Required to submit a detailed description of the language assistance services they will provide to LEP persons to ensure meaningful access to their programs and/or services, within ten (10) days of the date the contract is approved by Governor and Council; and
 - 3.17.5.6.2. Monitored on their Federal civil rights compliance using the Federal Civil Rights Compliance Checklist, which can be found in the Vendor/RFP section of the Department's website.
- 3.17.5.7. The guidance that accompanies Title VI of the Civil Rights Act of 1964 requires recipients to take reasonable steps to ensure meaningful access to their programs and services by persons with Limited English Proficiency (LEP persons). The extent of an organization's obligation to provide LEP services is based on an individualized assessment involving the balancing of four factors:
 - 3.17.5.7.1. The number or proportion of LEP persons served or likely to be encountered in the population that is eligible for the program or services (this includes minor children served by the program who have LEP parent(s) or guardian(s) in need of language assistance);
 - 3.17.5.7.2. The frequency with which LEP individuals come in contact with the program, activity or service;
 - 3.17.5.7.3. The importance or impact of the contact upon the lives of the person(s) served by the program, activity or service; and
 - 3.17.5.7.4. The resources available to the organization to provide language assistance.



- 3.17.5.8. **Contractors are required to complete the TWO (2) steps listed in the Appendix C to this RFP, as part of their Proposal.** Completion of these two items is required not only because the provision of language and/or communication assistance is a longstanding requirement under the Federal civil rights laws, but also because consideration of all the required factors will help inform Vendors' program design, which in turn, will allow Vendors to put forth the best possible Proposal.
- 3.17.5.9. For guidance on completing the two steps in Appendix C, please refer to Proposer's Reference for Completing the CLAS Section of the RFP, which is posted on the Department's website.
<http://www.dhhs.nh.gov/business/forms.htm>.

3.17.6. Audit Requirements

- 3.17.6.1. The Contractor is required to submit an annual audit to the Department if **any** of the following conditions exist:
- 3.17.6.1.1. Condition A - The Contractor expended \$750,000 or more in federal funds received as a subrecipient pursuant to 2 CFR Part 200, during the most recently completed fiscal year.
 - 3.17.6.1.2. Condition B - The Contractor is subject to audit pursuant to the requirements of NH RSA 7:28, III-b, pertaining to charitable organizations receiving support of \$1,000,000 or more.
 - 3.17.6.1.3. Condition C - The Contractor is a public company and required by Security and Exchange Commission (SEC) regulations to submit an annual financial audit.
- 3.17.6.2. If Condition A exists, the Contractor shall submit an annual **single audit** performed by an independent Certified Public Accountant (CPA) to the Department within 120 days after the close of the Contractor's fiscal year, conducted in accordance with the requirements of 2 CFR Part 200, Subpart F of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal awards.
- 3.17.6.3. If Condition B or Condition C exists, the Contractor shall submit an annual **financial audit** performed by an independent CPA within 120 days after the close of the Contractor's fiscal year.



- 3.17.6.4. Any Contractor that receives an amount equal to or greater than \$250,000 from the Department during a single fiscal year, regardless of the funding source, may be required, at a minimum, to submit annual financial audits performed by an independent CPA if the Department's risk assessment determination indicates the Contractor is high-risk.
- 3.17.6.5. In addition to, and not in any way in limitation of obligations of the Contract, it is understood and agreed by the Contractor that the Contractor shall be held liable for any state or federal audit exceptions and shall return to the Department all payments made under the Contract to which exception has been taken, or which have been disallowed because of such an exception.

3.18. Contract Monitoring Provisions

- 3.18.1. All Contractors must complete Appendix B, Contract Monitoring Provisions
- 3.18.2. The Department will use Vendor responses to conduct a risk assessment to determine if enhanced contract monitoring is necessary if the Vendor is awarded a contract. The risk assessment will not be used to disqualify or score Proposals.
- 3.18.3. The Department will complete the risk assessment utilizing multiple factors that include, but are not limited to:
 - 3.18.3.1. Grant management experience.
 - 3.18.3.2. Documented history of non-performance or non-compliance.
 - 3.18.3.3. Audit findings.
 - 3.18.3.4. Recent personnel or system changes.
 - 3.18.3.5. Financial solvency.
 - 3.18.3.6. Adequacy of internal controls.
- 3.18.4. The Department may incorporate contract monitoring procedures and activities into the final contract to address identified risks, which may include but are not limited to:
 - 3.18.4.1. Requiring the Contractor to provide fiscal reports and documentation behind reports to the Department for review.
 - 3.18.4.2. Reviewing Contractor reporting processes and systems for data integrity.
 - 3.18.4.3. Performing file reviews to ensure Contractor compliance with state and federal laws and rules in the administration of the contract.



- 3.18.4.4. Conducting site visits to assess Contractor compliance with applicable contract objectives and requirements.
- 3.18.4.5. Reviewing Contractor expenditure details to ensure all expenditures are allowable and in compliance with federal and state laws and other applicable policies or rules.
- 3.18.4.6. Providing targeted training or technical assistance to the Contractor.
- 3.18.4.7. Reviewing monthly financial data to assess Contractor financial solvency.

3.18.5. Statement of Vendor's Financial Condition

- 3.18.5.1. The Proposer's ability to demonstrate adequate financial resources for performance of the contract or the ability to obtain such resources as required during performance under this contract will be considered by the Department as part of the risk assessment to determine if enhanced contract monitoring is required if a contract is awarded.
- 3.18.5.2. Each Proposer must submit audited financial statements for the four (4) most recently completed fiscal years. Statements must include a report by an independent auditor that expresses an unqualified or qualified opinion as to whether the accompanying financial statements are presented fairly in accordance with generally accepted accounting principles.
- 3.18.5.3. Complete financial statements must include the following:
 - 3.18.5.3.1. Opinion of Certified Public Accountant;
 - 3.18.5.3.2. Balance Sheet;
 - 3.18.5.3.3. Income Statement;
 - 3.18.5.3.4. Statement of Cash Flow;
 - 3.18.5.3.5. Statement of Stockholder's Equity of Fund Balance;
 - 3.18.5.3.6. Complete Financial Notes; and
 - 3.18.5.3.7. Consolidating and Supplemental Financial Schedules.



- 3.18.5.4. A Proposer, which is part of a consolidated financial statement, may file the audited consolidated financial statements if it includes the consolidating schedules as supplemental information. A Proposer, which is part of a consolidated financial statement, but whose certified consolidated financial statements do not contain the consolidating schedules as supplemental information, shall, in addition to the audited consolidated financial statements, file unaudited financial statements for the Vendor alone accompanied by a certificate of authenticity signed by an officer of the corporation, partner, or owner under penalty of unsworn falsification which attests that the financial statements are correct in all material respects.
- 3.18.5.5. If a Proposer is not otherwise required by either state or federal statute to obtain a certification of audit of its financial statements, and thereby elects not to obtain such certification of audit, the Proposer shall submit the following as part of its proposal:
 - 3.18.5.5.1. Uncertified financial statements; and
 - 3.18.5.5.2. A certificate of authenticity which attests that the financial statements are correct in all material respects and is signed by an officer of the corporation, partner, or owner under penalty of unsworn falsification.

4. FINANCE

4.1. Financial Standards

4.1.1. Financial Funding Sources

- 4.1.1.1. The Department anticipates using Federal and General funds for the resulting contract(s). The Department may choose to modify the source of funding contingent upon the availability of funds at the time of award. Any selected vendor will be subject to the requirements in the Catalog of Federal Domestic Assistance (CFDA) # 93.563, U.S. Department of Health and Human Services, Administration for Children Youth and Families, Child Support Enforcement.

4.1.2. Price Schedule

- 4.1.2.1. The selected Vendor must provide services under the resulting contract based on all-inclusive fixed price per transaction and/or prices for all other services and products offered by the selected Vendor and must be presented in the form of a proposed Appendix D, Price Schedule. The price



of an annual SSAE No. 16 Audit and the total price of the audits during the term of the resulting contract must be identified as a separate line item in the Price Schedule. The final Price Schedule, incorporated into the resulting contract, is subject to Department approval.

- 4.1.2.2. The selected Vendor understands and agrees that the cost structure, including the unit prices specified in Appendix D, Price Schedule, are guaranteed for the Contract Period of the resulting contract, as specified in subsection 1.3, Contract Period, except that a price change may be negotiated if one or both of the following occurs:
 - 4.1.2.2.1. Unanticipated changes in the US Postal Service rate; or
 - 4.1.2.2.2. BCSS requests a change in the Scope of Services to be performed.
 - 4.1.2.2.3. Invoicing.
- 4.1.2.3. The selected Vendor will invoice BCSS monthly for services performed in accordance with the resulting contract. The selected Vendor must ensure BCSS receives the applicable invoice within thirty (30) days following the end of the month in which services were provided.
- 4.1.2.4. The selected Vendor must ensure invoices identify the following:
 - 4.1.2.4.1. Itemization of all units of service and prices charged to BCSS (formatted pursuant to the Price Schedule in Appendix D);
 - 4.1.2.4.2. Total price;
 - 4.1.2.4.3. Any earnings credit;
 - 4.1.2.4.4. Net balance for charges (total price less earnings credit); and
 - 4.1.2.4.5. Other information as mutually agreed upon by both parties.
- 4.1.2.5. The selected Vendor must ensure invoices include an itemization of prices charged for EFT/EDI, which includes:
 - 4.1.2.5.1. An itemization of all units of services and prices, including any and all specified prices pertaining to the processing of EFT/EDI;
 - 4.1.2.5.2. The total price for all EFT/EDI services; and



- 4.1.2.5.3. An itemized Monthly Fees portion that includes: data output fee; transaction fee with the number of transactions; and ACH items returned fee with the number of returned items.

- 4.1.2.6. Posting Errors

- 4.1.2.6.1. The selected Vendor must reimburse the Department for errors made by the Vendor in recording or posting payments that result in incorrect distributions. BCSS will provide written notice of the Vendor's errors. The notice will specify the amount, date, Social Security Number and Case Identification Number and/or Payor Identification Number.

- 4.1.2.6.2. The cost of the Vendor's posting errors will be borne by the selected Vendor. The Department will collect on these costs by deducting the amount owed by the selected Vendor from the selected Vendor's future invoice.

- 4.1.2.7. Non-Sufficient Fund Check Fees and Associated Costs

- 4.1.2.7.1. Fees and associated costs, charged by the bank in which the dedicated SDU-BCSS bank account is held, for Non-Sufficient Fund checks presented for payment and deposit by the selected Vendor will be charged directly to BCSS by the bank.

- 4.1.2.7.2. Fees and associated costs incurred by BCSS for Non-Sufficient Fund checks presented for deposit after receiving BCSS notice pursuant to subsection 3.3.6.10, will be borne by the selected Vendor as follows: an amount, including the amount of the check and all fees and associated costs charged by the bank, will be deducted by BCSS from the selected Vendor's monthly invoice as a credit toward the amount owed by BCSS to the selected Vendor for the applicable month. The selected Vendor will accordingly credit BCSS this amount.

- 4.1.3. **Statements**

- 4.1.3.1. The selected Vendor must provide an itemized statement of services rendered to each individual account in the prior month, to BCSS no later than the fifteenth (15th) day of the following month. Itemized statements must include



payments received and credited to each account for the previous month. Additionally, the monthly, itemized statement must include: the date of receipt; the check number; the amount of the payment; and the source of the payment.

4.1.4. Financial Management

- 4.1.4.1. The selected Vendor will designate a contact person to resolve any questions or discrepancies regarding invoices. The selected Vendor must provide BCSS with the name; title; telephone number; fax number; and email address of the contact person. The selected Vendor must notify BCSS in the event of a change of the designated contact person.
- 4.1.4.2. The Department will provide the selected Vendor with the name, title, mailing address and telephone number of the corresponding BCSS contact person. The Department will notify the selected Vendor in the event of a change in the designated contact person.

4.1.5. Payment

- 4.1.5.1. BCSS may withhold ten percent (10%) of a monthly payment for services performed under the contract if, in the sole judgment of BCSS, the selected Vendor is non-compliant with the terms and conditions of the contract and/or the Scope of Work, including but not limited to: quality of SDU and EFT services; quantity of SDU and EFT services; accuracy of service delivery and transaction processing; timeliness of service delivery and transaction processing; and security requirements. BCSS will provide the selected Vendor with a written list of specific services, transactions or conditions requiring correction or remediation. Payments withheld by BCSS may be released upon determination by BCSS that the conditions causing non-compliance have been corrected and remedied to the satisfaction of BCSS.

4.2. Budget, Staff List and Budget Narrative

- 4.2.1. Cost Proposals will be analyzed and normalized. For example, if a particular proposal would impose costs on the Department, that cost will be identified, assigned a monetary value, and that value will be added to the Bidder's proposed cost before scoring. Once all cost proposals have been normalized, each adjusted cost figure will be scored using the following formula:
- 4.2.2. Bidder's Cost Score = (Lowest Adjusted Proposed Cost / Bidder's Adjusted Proposed Cost) multiplied by four hundred twenty-five (425) points.



- 4.2.3. For the purpose of this formula, the lowest proposed adjusted cost is defined as the lowest adjusted cost proposed by a bidder whose proposal fulfills the minimum established qualifications. For example, if there were three valid bids with adjusted costs as shown in the first column of Table 1, the points awarded for the respective cost proposals are shown in the third column.

Table 1

Adjusted Cost Proposal	Calculation Formula	Score Points Awarded
\$100,000	$\$100,000 / \$100,000 \times 425$	425
\$120,000	$\$100,000 / \$120,000 \times 425$	353
\$150,000	$\$100,000 / \$150,000 \times 425$	285

5. PROPOSAL EVALUATION

5.1. Selection

- 5.1.1. The Department will use a scoring scale of 1280 points, with a maximum of 425 points awarded based on the Cost Proposal. The Department will select a Vendor based upon the criteria and standards contained in this RFP and applying the points set forth below.

5.2. Technical Proposal

- | | |
|---|-----------|
| 5.2.1. Operation Site (Q1) | 40 Points |
| 5.2.2. Processing payments received (Q2) | 40 Points |
| 5.2.3. Disbursed payments (Q3) | 40 Points |
| 5.2.4. Cardholder Terms (Q4) | 35 Points |
| 5.2.5. ATM Network (Q5) | 35 Points |
| 5.2.6. Card acceptance (Q6) | 30 Points |
| 5.2.7. Teller Cash (Q7) | 30 Points |
| 5.2.8. Transaction Processing (Q8) | 40 Points |
| 5.2.9. Self-Service Web Portal (Q9) | 40 Points |
| 5.2.10. Notifications (Q10) | 30 Points |
| 5.2.11. Automated Response Unit (Q11) | 30 Points |
| 5.2.12. Identity verification (Q12) | 30 Points |
| 5.2.13. Cardholder Help Desk Requirements (Q13) | 20 Points |
| 5.2.14. Samples (Q14) | 15 Points |
| 5.2.15. Banking services requirements (Q15) | 20 Points |



5.2.16. Education and Training plan (Q16)	10 Points
5.2.17. Reporting (Q17)	20 Points
5.2.18. IT Solution (Appendix G responses)	350 Points

Total Technical Proposal Points Available 855 Points

5.3. Cost Proposal

Total Cost Proposal Points Available	425 Points
Maximum Possible Score	1280 Points

6. PROPOSAL PROCESS

6.1. Contact Information – Sole Point of Contact

- 6.1.1. The sole point of contact, the Contract Specialist, relative to the proposal process for this RFP, from the RFP issue date until the selection of a Proposer, and approval of the resulting contract by the Governor and Executive Council is:

State of New Hampshire
Department of Health and Human Services
Shannon DuBreuil
Bureau of Contracts & Procurements
129 Pleasant Street
Concord, New Hampshire 03301
Email: Shannon.DuBreuil@dhhs.nh.gov
Phone: 603-271-9615

- 6.1.2. From the date of release of this RFP until an award is made and announced regarding the selection of a Proposer, all communication with personnel employed by or under contract with the Department regarding this RFP is prohibited unless first approved by the RFP Sole Point of Contact listed in Section 6.1.1, herein. Department employees have been directed not to hold conferences and/or discussions concerning this RFP with any potential Contractor during the selection process, unless otherwise authorized by the RFP Sole Point of Contact. Proposers may be disqualified for violating this restriction on communications.



6.2. Procurement Timetable

<u>Procurement Timetable</u> (All times are according to Eastern Time. The Department reserves the right to modify these dates at its sole discretion.)		
Item	Action	Date
1.	Release RFP	April 8, 2021
2.	Optional Letter of Intent Submission Deadline	April 16, 2021
3.	RFP Questions Submission Deadline	April 26, 2021 2:00 PM
4.	Department Response to Questions Published	May 3, 2021
5.	Proposal Submission Deadline	June 7, 2021 11:59 PM

6.3. Letter of Intent

- 6.3.1. A Letter of Intent to submit a Proposal in response to this RFP is optional.
- 6.3.2. Receipt of the Letter of Intent by Department will be required to receive any correspondence regarding this RFP; any RFP amendments, in the event such are produced; or any further materials on this project, including electronic files containing tables required for response to this RFP; any addenda; corrections; schedule modifications; or notifications regarding any informational meetings for Vendors; or responses to comments; or questions.
- 6.3.3. The Letter of Intent must be transmitted by email to the Contract Specialist identified in Subsection 6.1.
- 6.3.4. The Proposer is responsible for successful email transmission. The Letter of Intent must include the name, telephone number, mailing address and email address of the Vendor's designated contact. The Department will provide confirmation of receipt of the Letter of Intent if the name and email address of the person to receive such confirmation is provided by the Vendor.
- 6.3.5. Notwithstanding the Letter of Intent, Vendors remain responsible for reviewing the most updated information related to this RFP before submitting a proposal.



6.4. Questions and Answers

6.4.1. Proposers' Questions

- 6.4.1.1. All questions about this RFP including, but not limited to, requests for clarification, additional information or any changes to the RFP must be made in writing, by email only, citing the RFP page number and part or subpart, and submitted to the Contract Specialist identified in Subsection 6.1.
- 6.4.1.2. The Department may consolidate or paraphrase questions for efficiency and clarity. Questions that are not understood will not be answered. Statements that are not questions will not receive a response.
- 6.4.1.3. The questions must be submitted by email; however, the Department assumes no liability for ensuring accurate and complete email transmissions.
- 6.4.1.4. Questions must be received by the Department by the deadline given in Subsection 6.2, Procurement Timetable.

6.4.2. Department Answers

The Department intends to issue responses to properly submitted questions by the deadline specified in Subsection 6.2, Procurement Timetable. All oral answers given are non-binding. Written answers to questions received will be posted on the Department's website at (<http://www.dhhs.nh.gov/business/rfp/index.htm>). Vendors will be sent an email to the contact identified in the Letters of Intent indicating that the Questions and Answers have been posted on the Department's website. This date may be subject to change at the Department's discretion.

6.5. Exceptions

- 6.5.1. The Department will require the successful Proposer to execute a contract using the Form P-37, General Provisions and Standard Exhibits, which are attached as Appendix A. To the extent that a Vendor believes that exceptions to Appendix A will be necessary for the Vendor to enter into a Contract, the Vendor must note those issues during the RFP Question Period in Subsection 6.2. Proposers may not request exceptions to the Scope of Services or any other sections of this RFP.
- 6.5.2. The Department will review requested exceptions and accept, reject or note that it is open to negotiation of the proposed exception at its sole discretion.



- 6.5.3. If the Department accepts a Proposer's exception, the Department will, at the conclusion of the RFP Question Period, provide notice to all potential Contractors of the exceptions that have been accepted and indicate that exception is available to all potential Contractors by publication of the Department's answers on or about the date indicated in Subsection 6.2.
- 6.5.4. Any exceptions to the standard form contract and exhibits that are not raised by a Proposer during the RFP Question Period will not be considered. In no event is a Vendor to submit its own standard contract terms and conditions as a replacement for the Department's terms in response to this solicitation.

6.6. RFP Amendment

The Department reserves the right to amend this RFP, as it deems appropriate prior to the Proposal Submission Deadline on its own initiative or in response to issues raised through Proposer questions. In the event of an amendment to the RFP, the Department, at its sole discretion, may extend the Proposal Submission Deadline. Proposer who submitted a Letter of Intent will receive notification of the amendment, and the amended language will be posted on the Department's website.

6.7. Proposal Submission

- 6.7.1. Proposals must be submitted electronically to contracts@dhhs.nh.gov and the Contract Specialist at the email address specified in Subsection 6.1.
 - 6.7.1.1. The subject line must include the following information: RFP-2022-DEHS-01-STATE (email xx of xx).
 - 6.7.1.2. The maximum size of file attachments per email is 10 MB. Proposals with file attachments exceeding 10 MB must be submitted via multiple emails.
- 6.7.2. The Department must receive the Proposal by the time and date specified in the Procurement Timetable in Section 6 and in the manner specified or it may be rejected as non-compliant, unless waived by the Department as a non-material deviation.
- 6.7.3. The Department will conduct an initial screening step to verify Proposer compliance with the submissions requirements of this RFP. The Department may waive or offer a limited opportunity for a Proposer to cure immaterial deviations from the RFP requirements if it is deemed to be in the best interest of the Department.
- 6.7.4. Late submissions that are not accepted will remain unopened. Disqualified submissions will be discarded. Submission of the Proposals shall be at the Proposer's expense.



6.8. Non-Collusion

The Proposer's required signature on the Transmittal Cover Letter for a Proposal submitted in response to this RFP guarantees that the prices, terms and conditions, and services quoted have been established without collusion with other vendors and without effort to preclude the Department from obtaining the best possible competitive proposal.

6.9. Collaborative Proposals

Proposals must be submitted by one organization. Any collaborating organization must be designated as a subcontractor subject to the terms of Appendix A, P-37 General Provisions and Standard Exhibits.

6.10. Validity of Proposals

Proposals must be valid for one hundred and eighty (180) days following the deadline for submission in the Procurement Timetable above in Subsection 6.2, or until the Effective Date of any resulting Contract, whichever is later.

6.11. Property of Department

All material property submitted and received in response to this RFP will become the property of the Department and will not be returned to the Proposer. The Department reserves the right to use any information presented in any Proposal provided that its use does not violate any copyrights or other provisions of law.

6.12. Proposal Withdrawal

Prior to the Proposal Submission Deadline specified in Subsection 6.2, Procurement Timetable, a submitted Letter of Intent or Proposal may be withdrawn by submitting a written request for its withdrawal to the Contract Specialist specified in Subsection 6.1.

6.13. Public Disclosure

- 6.13.1. Pursuant to RSA 21-G:37, the content of responses to this RFP must remain confidential until the Governor and Executive Council have awarded a contract. At the time of receipt of Proposals, the Department will post the number of responses received with no further information. No later than five (5) business days prior to submission of a contract to the Department of Administrative Services pursuant to this RFP, the Department will post the name, rank or score of each Proposer. The Proposer's disclosure or distribution of the contents of its Proposal, other than to the Department, will be grounds for disqualification at the Department's sole discretion.



- 6.13.2. The content of each Proposal and addenda thereto will become public information once the Governor and Executive Council have approved a contract. Any information submitted as part of a Proposal in response to this RFP may be subject to public disclosure under RSA 91-A. In addition, in accordance with RSA 9-F:1, any contract entered into as a result of this RFP will be made accessible to the public online via the website Transparent NH (www.nh.gov/transparentnh/). Accordingly, business financial information and proprietary information such as trade secrets, business and financials models and forecasts, and proprietary formulas may be exempt from public disclosure under RSA 91-A:5, IV.
- 6.13.3. Insofar as a Proposer seeks to maintain the confidentiality of its confidential commercial, financial or personnel information, the Proposer must clearly identify in writing the information it claims to be confidential and explain the reasons such information should be considered confidential. This must be done by separate letter identifying by page number and Proposal section the specific information the Vendor claims to be exempt from public disclosure pursuant to RSA 91-A:5. **The Proposer is strongly encouraged to provide a redacted copy of their Proposal.**
- 6.13.4. Each Proposer acknowledges that the Department is subject to the Right-to-Know Law New Hampshire RSA Chapter 91-A. The Department shall maintain the confidentiality of the identified confidential information insofar as it is consistent with applicable laws or regulations, including but not limited to New Hampshire RSA Chapter 91-A. In the event the Department receives a request for the information identified by a Proposer as confidential, the Department shall notify the Proposer and specify the date the Department intends to release the requested information. Any effort to prohibit or enjoin the release of the information shall be the Proposer's responsibility and at the Proposer's sole expense. If the Proposer fails to obtain a court order enjoining the disclosure, the Department may release the information on the date the Department specified in its notice to the Proposer without incurring any liability to the Proposer.

6.14. Non-Commitment

Notwithstanding any other provision of this RFP, this RFP does not commit the Department to award a contract. The Department reserves the right to reject any and all Proposals or any portions thereof, at any time and to cancel this RFP and to solicit new Proposals under a new procurement process.

6.15. Liability

By submitting a Proposal in response to this RFP, a Proposer agrees that in no event shall the Department be either responsible for or held liable for any costs incurred by a Proposer in the preparation or submittal of or otherwise in connection with a Proposal, or for work performed prior to the Effective Date of a resulting contract.



6.16. Request for Additional Information or Materials

The Department may request any Proposer to provide additional information or materials needed to clarify information presented in the Proposal. Such a request will be issued in writing and will not provide a Proposer with an opportunity to change, extend, or otherwise amend its Proposal in intent or substance.

6.17. Oral Presentations and Discussions

The Department reserves the right to require some or all Proposers to make oral presentations of their Proposal. The purpose of the oral presentation is to clarify and expound upon information provided in the written Proposal. Proposers are prohibited from altering the original substance of their Proposals during the oral presentations. The Department will use the information gained from oral presentations to refine the technical review scores. Any and all costs associated with an oral presentation shall be borne entirely by the Proposer.

6.18. Successful Proposer Notice and Contract Negotiations

- 6.18.1. If a Proposer is selected, the Department will send written notification of their selection and the Department's desire to enter into contract negotiations. Until the Department successfully completes negotiations with the selected Proposer(s), all submitted Proposals remain eligible for selection by the Department. In the event contract negotiations are unsuccessful with the selected Proposer(s), the evaluation team may recommend another Proposer(s). The Department will not contact Proposer(s) that are not initially selected to enter into contract negotiations.

6.19. Scope of Award and Contract Award Notice

- 6.19.1. The Department reserves the right to award a service, part of a service, group of services, or total Proposal and to reject any and all Proposals in whole or in part. A contract award is contingent on approval by the Governor and Executive Council.
- 6.19.2. If a contract is awarded, the Contractor must obtain written consent from the State before any public announcement or news release is issued pertaining to any contract award.

6.20. Site Visits

The Department may, at its sole discretion, at any time prior to contract award, conduct a site visit at the Proposer's location or at any other location deemed appropriate by the Department, to determine the Proposer's capacity to satisfy the terms of this RFP. The Department may also require the Proposer to produce additional documents, records, or materials relevant to determining the Proposer's capacity to satisfy the terms of this RFP. Any and all costs associated with any site visit or requests for documents shall be borne entirely by the Proposer.



6.21. Protest of Intended Award

Any challenge of an award made or otherwise related to this RFP shall be governed by RSA 21-G:37, and the procedures and terms of this RFP. The procedure set forth in RSA 21-G:37, IV, shall be the sole remedy available to challenge any award resulting from this RFP. In the event that any legal action is brought challenging this RFP and selection process, outside of the review process identified in RSA 21-G:37,IV, and in the event that the State of New Hampshire prevails, the challenger agrees to pay all expenses of such action, including attorney's fees and costs at all stages of litigation.

6.22. Contingency

Aspects of the award may be contingent upon changes to state or federal laws and regulations.

6.23. Ethical Requirements

From the time this RFP is published until a contract is awarded, no Proposer shall offer or give, directly or indirectly, any gift, expense reimbursement, or honorarium, as defined by RSA 15-B, to any elected official, public official, public employee, constitutional official, or family member of any such official or employee who will or has selected, evaluated, or awarded an RFP, or similar submission. Any Proposer that violates RSA 21-G:38 shall be subject to prosecution for an offense under RSA 640:2. Any Proposer who has been convicted of an offense based on conduct in violation of this section, which has not been annulled, or who is subject to a pending criminal charge for such an offense, shall be disqualified from submitting an Proposal to this RFP, or similar request for submission and every such Proposer shall be disqualified from submitting any Proposal or similar request for submission issued by any state agency. A Proposer that was disqualified under this section because of a pending criminal charge which is subsequently dismissed, results in an acquittal, or is annulled, may notify the Department of Administrative Services, which shall note that information on the list maintained on the state's internal intranet system, except in the case of annulment, the information, shall be deleted from the list.

7. PROPOSAL OUTLINE AND REQUIREMENTS

7.1. Presentation and Identification

7.1.1. Overview

- 7.1.1.1. Acceptable Proposals must offer all services identified in Section 3 - Statement of Work, unless an allowance for partial scope is specifically described in Section 3.
- 7.1.1.2. Proposals must be submitted electronically as specified in Subsection 6.7.
- 7.1.1.3. Proposers must submit a separate electronic document for the Technical Proposal and a separate electronic document for the Cost Proposal.



7.1.1.4. Fax or hard copies will not be accepted.

7.2. Outline and Detail

7.2.1. Proposal Contents – Outline

Each Proposal shall contain the following, in the order described in this section.

7.2.2. Technical Proposal Contents – The Transmittal Cover Letter must:

- 7.2.2.1. Be on the Proposer's company letterhead.
- 7.2.2.2. Be signed by an individual who is authorized to bind the company to all statements, including services and prices contained in the Proposal.
- 7.2.2.3. Contain the following:
 - 7.2.2.3.1. Identify the submitting organization;
 - 7.2.2.3.2. Identify the name, title, mailing address, telephone number and email address of the person authorized by the organization to contractually obligate the organization;
 - 7.2.2.3.3. Identify the name, title, mailing address, telephone number and email address of the fiscal agent of the organization;
 - 7.2.2.3.4. Identify the name, title, telephone number, and email address of the person who will serve as the Vendor's representative for all matters relating to the RFP;
 - 7.2.2.3.5. Acknowledge that the Proposer has read this RFP, understands it, and agrees to be bound by its requirements;
 - 7.2.2.3.6. Explicitly state acceptance of terms, conditions, and general instructions stated in Section 8 Mandatory Business Specifications;
 - 7.2.2.3.7. Confirm that Appendix A P-37 General Provisions and Standard Exhibits has been read and is understood;
 - 7.2.2.3.8. Explicitly state that the Proposal is valid for one hundred and eighty (180) days following the deadline for submission in the Procurement Timetable above in Subsection 6.2, or until the Effective Date of any resulting Contract, whichever is later; and
 - 7.2.2.3.9. Include the date that the Proposal was submitted.



7.2.3. Table of Contents

The required elements of the Proposal shall be numbered sequentially and represented in the Table of Contents.

7.2.4. Executive Summary. A Proposer must submit an executive summary to:

- 7.2.4.1. Provide the Department with an overview of the organization and what the Vendor intends to provide;
- 7.2.4.2. Demonstrate an understanding of the services requested in this RFP and any problems anticipated in accomplishing the work;
- 7.2.4.3. Demonstrate the overall design of the project in response to achieving the deliverables as defined in this RFP; and
- 7.2.4.4. Demonstrate familiarity with the project elements, its solutions to the problems presented and knowledge of the requested services.

7.2.5. Proposal Narrative, Project Approach, and Technical Response

- 7.2.5.1. The Proposer must answer all questions and must include all items requested for the Proposal to be considered. The Proposer must address every section of Section 3 Statement of Work.
- 7.2.5.2. Responses must be in the same sequence and format as listed in Section 3 Statement of Work and must, at a minimum, cite the relevant section, subsection, paragraph and subparagraph number, as appropriate.
- 7.2.5.3. Proposers are encouraged, but not required to include a Word version of the proposal narrative in the electronic copy.

7.2.6. Description of Organization

- 7.2.6.1. Proposers must include in their Proposal a summary of the company's organization, management and history and how the organization's experience demonstrates the ability to meet the needs of requirements in this RFP. At a minimum, the description must include:
 - 7.2.6.1.1. General company overview;
 - 7.2.6.1.2. Ownership and subsidiaries;
 - 7.2.6.1.3. Company background and primary lines of business;
 - 7.2.6.1.4. Number of employees;
 - 7.2.6.1.5. Headquarters and satellite locations;



- 7.2.6.1.6. Current project commitments;
- 7.2.6.1.7. Major government and private sector clients;
- 7.2.6.1.8. Mission Statement;
- 7.2.6.1.9. The programs and activities of the company;
- 7.2.6.1.10. The number of people served;
- 7.2.6.1.11. Company accomplishments;
- 7.2.6.1.12. Reasons the company is capable of effectively completing the services outlined in the RFP; and
- 7.2.6.1.13. All strengths considered to be assets to the company.

- 7.2.6.2. The Proposer should demonstrate the length, depth, and applicability of all prior experience in providing the requested services as well as the skill and experience of staff.

7.2.7. Proposer's References

- 7.2.7.1. The Proposal must include relevant information about at least three (3) similar or related contracts or subcontracts awarded to the Vendor. Particular emphasis should be placed on previous contractual experience with government agencies. The Department reserves the right to contact any reference identified. The information must contain the following:
 - 7.2.7.1.1. Name, address, telephone number, and website of the customer;
 - 7.2.7.1.2. A description of the work performed under each contract;
 - 7.2.7.1.3. A description of the nature of the relationship between the Vendor and the customer;
 - 7.2.7.1.4. Name and contact information of the person whom the Department can contact; and
 - 7.2.7.1.5. Dates of performance.

7.2.8. Subcontractor Letters of Commitment (if applicable)

The Proposer shall be solely responsible for meeting all requirements and terms and conditions specified in this RFP, its Proposal, and any resulting contract, regardless of whether it proposes to use any subcontractors. The Proposer and any subcontractors shall commit to the entire contract



period stated within the RFP, unless a change of subcontractors is specifically agreed to by the Department. All selected Contractor(s) that indicate an intention to subcontract must submit a subcontractor's letter of commitment to the Department no later than thirty (30) days from the contract effective date. The Department will approve or reject subcontractors for this project and require the Contractor to replace subcontractors found to be unacceptable.

7.2.9. New Hampshire Certificate of Good Standing

The Department requires, as applicable, every Contractor to acquire a Certificate of Good Standing or assurance of obtaining registration with the New Hampshire Office of the Secretary of State in accordance with RSA 5:18-a.

7.2.10. Affiliations – Conflict of Interest

The Proposer must include a statement regarding any and all affiliations that might result in a conflict of interest. Explain the relationship and how the affiliation would not represent a conflict of interest.

7.2.11. Required Attachments

7.2.11.1. The following are required statements that must be included with the Technical Proposal. The Proposer must complete the correlating forms found in the RFP Appendices and submit them as the "Required Attachments" section of the Technical Proposal.

7.2.11.1.1. Answers to questions in Section 3.

7.2.11.1.2. Appendix C, CLAS Requirements.

7.2.11.2. The following are required statements that must be included with the Cost Proposal. The Proposer must complete the correlating forms found in the RFP Appendices and submit them as the "Required Attachments" section of the Cost Proposal.

7.2.11.2.1. Audited financial statements identified in Paragraph 3.6.5

7.2.11.2.2. Appendix B, Contract Monitoring Provisions.

7.2.11.2.3. Appendix D, Price Schedule.

7.2.11.2.4. Appendix E, Program Staff List.

7.2.11.2.5. Budget Narrative.



8. MANDATORY BUSINESS SPECIFICATIONS

8.1. Contract Terms, Conditions and Liquidated Damages, Forms

8.1.1. Contract Terms and Conditions

The State of New Hampshire sample contract is attached. The Proposer must agree to contractual requirements as set forth in the Appendix A, P-37 General Provisions and Standard Exhibits.

8.1.2. Liquidated Damages

- 8.1.2.1. The Department may negotiate with the awarded vendor to include liquidated damages in the Contract in the event any deliverables are not met.
- 8.1.2.2. The Department and the Vendor agree that the actual damages that the Department will sustain in the event the Vendor fails to maintain the required performance standards throughout the life of the contract will be uncertain in amount and difficult and impracticable to determine. The Vendor acknowledges and agrees that any failure to achieve required performance levels by the Contractor will more than likely substantially delay and disrupt the Department's operations. Therefore, the parties agree that liquidated damages may be determined as part of the contract specifications.
- 8.1.2.3. Assessment of liquidated damages may be in addition to, and not in lieu of, such other remedies as may be available to the Department. Except and to the extent expressly provided herein, the Department shall be entitled to recover liquidated damages applicable to any given incident.
- 8.1.2.4. The Department may determine compliance and assessment of liquidated damages as often as it deems reasonable necessary to ensure required performance standards are met. Amounts due the Department as liquidated damages may be deducted by the Department from any fees payable to the Contractor and any amount outstanding over and above the amounts deducted from the invoice will be promptly tendered by check from the Contractor to the Department.



9. ADDITIONAL INFORMATION

- 9.1. Appendix A – Form P-37 General Provisions and Standard Exhibits**
- 9.2. Appendix B – Contract Monitoring Provisions**
- 9.3. Appendix C – CLAS Requirements**
- 9.4. Appendix D – Price Schedule**
- 9.5. Appendix E – Program Staff List**
- 9.6. Appendix F – Data Elements for Billing Coupons**
- 9.7. Appendix G – SDU Information Technology Provisions Statement of Work**
- 9.8. Appendix H – Technical Requirements Checklist**
- 9.9. Appendix I - Physical Security Requirements**
- 9.10. Appendix J – Required Data Elements for Payment Processing**
- 9.11. Appendix K – Statement on Standards for Attestation Engagements (SSAE 16)**
- 9.12. Appendix L – Corrective Action/Liquidated Damages Disclosure**

Do Not Return

Subject: _____

Notice: This agreement and all of its attachments shall become public upon submission to Governor and Executive Council for approval. Any information that is private, confidential or proprietary must be clearly identified to the agency and agreed to in writing prior to signing the contract.

AGREEMENT

The State of New Hampshire and the Contractor hereby mutually agree as follows:

GENERAL PROVISIONS**1. IDENTIFICATION.**

1.1 State Agency Name New Hampshire Department of Health and Human Services		1.2 State Agency Address 129 Pleasant Street Concord, NH 03301-3857	
1.3 Contractor Name 		1.4 Contractor Address 	
1.5 Contractor Phone Number () -	1.6 Account Number 	1.7 Completion Date Select a Date	1.8 Price Limitation
1.9 Contracting Officer for State Agency Nathan D. White, Director		1.10 State Agency Telephone Number (603) 271-9631	
1.11 Contractor Signature <div style="text-align: right;">Date:</div>		1.12 Name and Title of Contractor Signatory 	
1.13 State Agency Signature <div style="text-align: right;">Date:</div>		1.14 Name and Title of State Agency Signatory 	
1.15 Approval by the N.H. Department of Administration, Division of Personnel (if applicable) <div style="display: flex; justify-content: space-between;"> By: Director, On: </div>			
1.16 Approval by the Attorney General (Form, Substance and Execution) (if applicable) <div style="display: flex; justify-content: space-between;"> By: On: </div>			
1.17 Approval by the Governor and Executive Council (if applicable) <div style="display: flex; justify-content: space-between;"> G&C Item number: G&C Meeting Date: </div>			

Do Not Return

Page 1 of 4

 Contractor Initials _____
 Date _____

Do Not Return

2. SERVICES TO BE PERFORMED. The State of New Hampshire, acting through the agency identified in block 1.1 (“State”), engages contractor identified in block 1.3 (“Contractor”) to perform, and the Contractor shall perform, the work or sale of goods, or both, identified and more particularly described in the attached EXHIBIT B which is incorporated herein by reference (“Services”).

3. EFFECTIVE DATE/COMPLETION OF SERVICES.

3.1 Notwithstanding any provision of this Agreement to the contrary, and subject to the approval of the Governor and Executive Council of the State of New Hampshire, if applicable, this Agreement, and all obligations of the parties hereunder, shall become effective on the date the Governor and Executive Council approve this Agreement as indicated in block 1.17, unless no such approval is required, in which case the Agreement shall become effective on the date the Agreement is signed by the State Agency as shown in block 1.13 (“Effective Date”).

3.2 If the Contractor commences the Services prior to the Effective Date, all Services performed by the Contractor prior to the Effective Date shall be performed at the sole risk of the Contractor, and in the event that this Agreement does not become effective, the State shall have no liability to the Contractor, including without limitation, any obligation to pay the Contractor for any costs incurred or Services performed. Contractor must complete all Services by the Completion Date specified in block 1.7.

4. CONDITIONAL NATURE OF AGREEMENT.

Notwithstanding any provision of this Agreement to the contrary, all obligations of the State hereunder, including, without limitation, the continuance of payments hereunder, are contingent upon the availability and continued appropriation of funds affected by any state or federal legislative or executive action that reduces, eliminates or otherwise modifies the appropriation or availability of funding for this Agreement and the Scope for Services provided in EXHIBIT B, in whole or in part. In no event shall the State be liable for any payments hereunder in excess of such available appropriated funds. In the event of a reduction or termination of appropriated funds, the State shall have the right to withhold payment until such funds become available, if ever, and shall have the right to reduce or terminate the Services under this Agreement immediately upon giving the Contractor notice of such reduction or termination. The State shall not be required to transfer funds from any other account or source to the Account identified in block 1.6 in the event funds in that Account are reduced or unavailable.

5. CONTRACT PRICE/PRICE LIMITATION/ PAYMENT.

5.1 The contract price, method of payment, and terms of payment are identified and more particularly described in EXHIBIT C which is incorporated herein by reference.

5.2 The payment by the State of the contract price shall be the only and the complete reimbursement to the Contractor for all expenses, of whatever nature incurred by the Contractor in the performance hereof, and shall be the only and the complete

compensation to the Contractor for the Services. The State shall have no liability to the Contractor other than the contract price.

5.3 The State reserves the right to offset from any amounts otherwise payable to the Contractor under this Agreement those liquidated amounts required or permitted by N.H. RSA 80:7 through RSA 80:7-c or any other provision of law.

5.4 Notwithstanding any provision in this Agreement to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments authorized, or actually made hereunder, exceed the Price Limitation set forth in block 1.8.

6. COMPLIANCE BY CONTRACTOR WITH LAWS AND REGULATIONS/ EQUAL EMPLOYMENT OPPORTUNITY.

6.1 In connection with the performance of the Services, the Contractor shall comply with all applicable statutes, laws, regulations, and orders of federal, state, county or municipal authorities which impose any obligation or duty upon the Contractor, including, but not limited to, civil rights and equal employment opportunity laws. In addition, if this Agreement is funded in any part by monies of the United States, the Contractor shall comply with all federal executive orders, rules, regulations and statutes, and with any rules, regulations and guidelines as the State or the United States issue to implement these regulations. The Contractor shall also comply with all applicable intellectual property laws.

6.2 During the term of this Agreement, the Contractor shall not discriminate against employees or applicants for employment because of race, color, religion, creed, age, sex, handicap, sexual orientation, or national origin and will take affirmative action to prevent such discrimination.

6.3. The Contractor agrees to permit the State or United States access to any of the Contractor’s books, records and accounts for the purpose of ascertaining compliance with all rules, regulations and orders, and the covenants, terms and conditions of this Agreement.

7. PERSONNEL.

7.1 The Contractor shall at its own expense provide all personnel necessary to perform the Services. The Contractor warrants that all personnel engaged in the Services shall be qualified to perform the Services, and shall be properly licensed and otherwise authorized to do so under all applicable laws.

7.2 Unless otherwise authorized in writing, during the term of this Agreement, and for a period of six (6) months after the Completion Date in block 1.7, the Contractor shall not hire, and shall not permit any subcontractor or other person, firm or corporation with whom it is engaged in a combined effort to perform the Services to hire, any person who is a State employee or official, who is materially involved in the procurement, administration or performance of this Agreement. This provision shall survive termination of this Agreement.

7.3 The Contracting Officer specified in block 1.9, or his or her successor, shall be the State’s representative. In the event of any dispute concerning the interpretation of this Agreement, the Contracting Officer’s decision shall be final for the State.

Do Not Return

Contractor Initials _____

Date _____

Do Not Return**8. EVENT OF DEFAULT/REMEDIES.**

8.1 Any one or more of the following acts or omissions of the Contractor shall constitute an event of default hereunder ("Event of Default"):

8.1.1 failure to perform the Services satisfactorily or on schedule;

8.1.2 failure to submit any report required hereunder; and/or

8.1.3 failure to perform any other covenant, term or condition of this Agreement.

8.2 Upon the occurrence of any Event of Default, the State may take any one, or more, or all, of the following actions:

8.2.1 give the Contractor a written notice specifying the Event of Default and requiring it to be remedied within, in the absence of a greater or lesser specification of time, thirty (30) days from the date of the notice; and if the Event of Default is not timely cured, terminate this Agreement, effective two (2) days after giving the Contractor notice of termination;

8.2.2 give the Contractor a written notice specifying the Event of Default and suspending all payments to be made under this Agreement and ordering that the portion of the contract price which would otherwise accrue to the Contractor during the period from the date of such notice until such time as the State determines that the Contractor has cured the Event of Default shall never be paid to the Contractor;

8.2.3 give the Contractor a written notice specifying the Event of Default and set off against any other obligations the State may owe to the Contractor any damages the State suffers by reason of any Event of Default; and/or

8.2.4 give the Contractor a written notice specifying the Event of Default, treat the Agreement as breached, terminate the Agreement and pursue any of its remedies at law or in equity, or both.

8.3. No failure by the State to enforce any provisions hereof after any Event of Default shall be deemed a waiver of its rights with regard to that Event of Default, or any subsequent Event of Default. No express failure to enforce any Event of Default shall be deemed a waiver of the right of the State to enforce each and all of the provisions hereof upon any further or other Event of Default on the part of the Contractor.

9. TERMINATION.

9.1 Notwithstanding paragraph 8, the State may, at its sole discretion, terminate the Agreement for any reason, in whole or in part, by thirty (30) days written notice to the Contractor that the State is exercising its option to terminate the Agreement.

9.2 In the event of an early termination of this Agreement for any reason other than the completion of the Services, the Contractor shall, at the State's discretion, deliver to the Contracting Officer, not later than fifteen (15) days after the date of termination, a report ("Termination Report") describing in detail all Services performed, and the contract price earned, to and including the date of termination. The form, subject matter, content, and number of copies of the Termination Report shall be identical to those of any Final Report described in the attached EXHIBIT B. In addition, at the State's discretion, the Contractor shall, within 15 days of notice of early termination, develop and

submit to the State a Transition Plan for services under the Agreement.

10. DATA/ACCESS/CONFIDENTIALITY/PRESERVATION.

10.1 As used in this Agreement, the word "data" shall mean all information and things developed or obtained during the performance of, or acquired or developed by reason of, this Agreement, including, but not limited to, all studies, reports, files, formulae, surveys, maps, charts, sound recordings, video recordings, pictorial reproductions, drawings, analyses, graphic representations, computer programs, computer printouts, notes, letters, memoranda, papers, and documents, all whether finished or unfinished.

10.2 All data and any property which has been received from the State or purchased with funds provided for that purpose under this Agreement, shall be the property of the State, and shall be returned to the State upon demand or upon termination of this Agreement for any reason.

10.3 Confidentiality of data shall be governed by N.H. RSA chapter 91-A or other existing law. Disclosure of data requires prior written approval of the State.

11. CONTRACTOR'S RELATION TO THE STATE. In the performance of this Agreement the Contractor is in all respects an independent contractor, and is neither an agent nor an employee of the State. Neither the Contractor nor any of its officers, employees, agents or members shall have authority to bind the State or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

12. ASSIGNMENT/DELEGATION/SUBCONTRACTS.

12.1 The Contractor shall not assign, or otherwise transfer any interest in this Agreement without the prior written notice, which shall be provided to the State at least fifteen (15) days prior to the assignment, and a written consent of the State. For purposes of this paragraph, a Change of Control shall constitute assignment. "Change of Control" means (a) merger, consolidation, or a transaction or series of related transactions in which a third party, together with its affiliates, becomes the direct or indirect owner of fifty percent (50%) or more of the voting shares or similar equity interests, or combined voting power of the Contractor, or (b) the sale of all or substantially all of the assets of the Contractor.

12.2 None of the Services shall be subcontracted by the Contractor without prior written notice and consent of the State. The State is entitled to copies of all subcontracts and assignment agreements and shall not be bound by any provisions contained in a subcontract or an assignment agreement to which it is not a party.

13. INDEMNIFICATION. Unless otherwise exempted by law, the Contractor shall indemnify and hold harmless the State, its officers and employees, from and against any and all claims, liabilities and costs for any personal injury or property damages, patent or copyright infringement, or other claims asserted against the State, its officers or employees, which arise out of (or which may be claimed to arise out of) the acts or omission of the

Do Not Return

Contractor Initials _____

Date _____

Do Not Return

Contractor, or subcontractors, including but not limited to the negligence, reckless or intentional conduct. The State shall not be liable for any costs incurred by the Contractor arising under this paragraph 13. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

14. INSURANCE.

14.1 The Contractor shall, at its sole expense, obtain and continuously maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force, the following insurance:

14.1.1 commercial general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$1,000,000 per occurrence and \$2,000,000 aggregate or excess; and

14.1.2 special cause of loss coverage form covering all property subject to subparagraph 10.2 herein, in an amount not less than 80% of the whole replacement value of the property.

14.2 The policies described in subparagraph 14.1 herein shall be on policy forms and endorsements approved for use in the State of New Hampshire by the N.H. Department of Insurance, and issued by insurers licensed in the State of New Hampshire.

14.3 The Contractor shall furnish to the Contracting Officer identified in block 1.9, or his or her successor, a certificate(s) of insurance for all insurance required under this Agreement. Contractor shall also furnish to the Contracting Officer identified in block 1.9, or his or her successor, certificate(s) of insurance for all renewal(s) of insurance required under this Agreement no later than ten (10) days prior to the expiration date of each insurance policy. The certificate(s) of insurance and any renewals thereof shall be attached and are incorporated herein by reference.

15. WORKERS' COMPENSATION.

15.1 By signing this agreement, the Contractor agrees, certifies and warrants that the Contractor is in compliance with or exempt from, the requirements of N.H. RSA chapter 281-A ("*Workers' Compensation*").

15.2 To the extent the Contractor is subject to the requirements of N.H. RSA chapter 281-A, Contractor shall maintain, and require any subcontractor or assignee to secure and maintain, payment of Workers' Compensation in connection with activities which the person proposes to undertake pursuant to this Agreement. The Contractor shall furnish the Contracting Officer identified in block 1.9, or his or her successor, proof of Workers' Compensation in the manner described in N.H. RSA chapter 281-A and any applicable renewal(s) thereof, which shall be attached and are incorporated herein by reference. The State shall not be responsible for payment of any Workers' Compensation premiums or for any other claim or benefit for Contractor, or any subcontractor or employee of Contractor, which might arise under applicable State of New Hampshire Workers' Compensation laws in connection with the performance of the Services under this Agreement.

16. NOTICE. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses given in blocks 1.2 and 1.4, herein.

17. AMENDMENT. This Agreement may be amended, waived or discharged only by an instrument in writing signed by the parties hereto and only after approval of such amendment, waiver or discharge by the Governor and Executive Council of the State of New Hampshire unless no such approval is required under the circumstances pursuant to State law, rule or policy.

18. CHOICE OF LAW AND FORUM. This Agreement shall be governed, interpreted and construed in accordance with the laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their respective successors and assigns. The wording used in this Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party. Any actions arising out of this Agreement shall be brought and maintained in New Hampshire Superior Court which shall have exclusive jurisdiction thereof.

19. CONFLICTING TERMS. In the event of a conflict between the terms of this P-37 form (as modified in EXHIBIT A) and/or attachments and amendment thereof, the terms of the P-37 (as modified in EXHIBIT A) shall control.

20. THIRD PARTIES. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

21. HEADINGS. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

22. SPECIAL PROVISIONS. Additional or modifying provisions set forth in the attached EXHIBIT A are incorporated herein by reference.

23. SEVERABILITY. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

24. ENTIRE AGREEMENT. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire agreement and understanding between the parties, and supersedes all prior agreements and understandings with respect to the subject matter hereof.

Do Not Return

Contractor Initials _____

Date _____

EXHIBIT A

Revisions to Standard Agreement Provisions

1. Revisions to Form P-37, General Provisions

- 1.1. Paragraph 3, Subparagraph 3.1, Effective Date/Completion of Services, is amended as follows:
 - 3.1. Notwithstanding any provision of this Agreement to the contrary, and subject to the approval of the Governor and Executive Council of the State of New Hampshire as indicated in block 1.17, this Agreement, and all obligations of the parties hereunder, shall become effective upon Governor and Executive Council approval ("Effective Date").
- 1.2. Paragraph 3, Effective Date/Completion of Services, is amended by adding subparagraph 3.3 as follows:
 - 3.3. The parties may extend the Agreement for up to five (5) additional years from the Completion Date, contingent upon satisfactory delivery of services, available funding, agreement of the parties, and approval of the Governor and Executive Council.
- 1.3. Paragraph 5, Contract Price/Price Limitation/ Payment, is amended by adding subparagraph 5.5 to read:
 - 5.5 The State's liability under this Agreement shall be limited to monetary damages not to exceed the contract price pursuant to Paragraph 5.2. The Contractor agrees that it has an adequate remedy at law for any breach of this Agreement by the State and hereby waives any right to specific performance or other equitable remedies against the State. Subject to applicable laws and regulations, in no event shall the State be liable for any consequential, special, indirect, incidental, punitive, or exemplary damages. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State.
- 1.4. Paragraph 8, Event of Default/Remedies, is amended by adding subparagraph 8.4 to read:
 - 8.4 Procure Services that are the subject of the Contract from another source and Contractor shall be liable for reimbursing the State for the replacement Services, and all administrative costs directly related to the replacement of the Contract and procuring the Services from another source, such as costs of competitive bidding, mailing, advertising, applicable fees, charges or penalties, and staff time costs; all of which shall be subject to the limitations of liability set forth in the Contract.

EXHIBIT A

1.5. Paragraph 9, termination is amended to read:

9. TERMINATION

9.1 Notwithstanding paragraph 8, the State may, at its sole discretion, terminate the Agreement for any reason, in whole or in part. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. The State shall be liable for cost of all Services and Deliverables for which Acceptance has been given by the State, provided through the date of termination but will not be liable for any costs for incomplete Services or winding down the Contract activities. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

9.2 Termination Procedure

9.2.1 Upon termination of the Contract, the State, in addition to any other rights provided in the Contract, may require Contractor to deliver to the State any property, including without limitation, Software and Written Deliverables, for such part of the Contract as has been terminated.

9.2.2 After receipt of a notice of termination, and except as otherwise directed by the State, Contractor shall:

9.2.2.1 Stop work under the Contract on the date, and to the extent specified, in the notice;

9.2.2.2 Promptly, but in no event longer than ten (10) days after termination, terminate its orders and subcontracts related to the work which has been terminated, and settle all outstanding liabilities and all claims arising out of such termination of orders and subcontracts, with the approval or ratification of the State to the extent required, which approval or ratification shall be final for the purpose of this Section;

9.2.2.3 Take such action as the State directs, or as necessary to preserve and protect the property related to the Contract which is in the possession of Contractor and in which the State has an interest;

9.2.2.4 Take no action to intentionally erase any State data until directed by the State;

9.2.2.5 Transfer title to the State and deliver in the manner, at the times, and to the extent directed by the State, any property

EXHIBIT A

which is required to be furnished to the State and which has been accepted or requested by the State;

9.2.2.6 Implement an orderly return of State data in a CSV or another mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of State data;

9.2.2.7 Securely dispose of all requested data in all of its forms, such as disk, CD / DVD, backup tape and paper, when requested by the State. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-Special Publication (SP) 800-88 approved methods. Certificates of destruction shall be provided to the State; and

9.2.2.8 Provide written Certification to the State that Contractor has surrendered to the State all said property and after 180 days has erased all State data.

9.2.3 If the Contract has expired, or terminated prior to the Completion Date, for any reason, the Contractor shall provide, for a period up to ninety (90) days after the expiration or termination, all transition services requested by the State, at no additional cost, to allow for the expired or terminated portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees ("Transition Services").

9.2.4 This covenant in paragraph 9 shall survive the termination of this Contract.

1.6. Paragraph 10, Data/Access/Confidentiality/Preservation, is amended by adding the following:

10.4 In performing its obligations under this Agreement, Contractor may gain access to Confidential Information of the State. Confidential Information includes any and all information owned or managed by the State of NH - created, received from or on behalf of any Agency of the State or accessed in the course of performing contracted Services - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personally Identifiable Information (PII), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and Confidential Information. The Contractor shall not use the Confidential Information developed or obtained during the

EXHIBIT A

performance of, or acquired, or developed by reason of the Agreement, except as directly connected to and necessary for the performance of the Agreement. Contractor shall maintain the confidentiality of and protect from unauthorized use, disclosure, publication, and reproduction (collectively "release"), all Confidential Information.

- 10.4.1 In the event of the unauthorized release of Confidential Information, Contractor shall immediately notify the State, and the State may immediately be entitled to pursue any remedy at law and in equity, including, but not limited to, injunctive relief.
- 10.5 Subject to applicable federal or State laws and regulations, Confidential Information shall not include information which:
 - 10.5.1. shall have otherwise become publicly available other than as a result of disclosure by the receiving Party in breach hereof;
 - 10.5.2. was disclosed to the receiving Party on a non-confidential basis from a source other than the disclosing Party, which the receiving Party believes is not prohibited from disclosing such information as a result of an obligation in favor of the disclosing Party;
 - 10.5.3. is developed by the receiving Party independently of, or was known by the receiving Party prior to, any disclosure of such information made by the disclosing Party; or
 - 10.5.4. is disclosed with the written consent of the disclosing Party.
- 10.6 A receiving Party also may disclose Confidential Information to the extent required by an order of a court of competent jurisdiction. Any disclosure of the Confidential Information shall require the prior written approval of the State. Contractor shall immediately notify the State if any request, subpoena or other legal process is served upon Contractor regarding the Confidential Information, and Contractor shall cooperate with the State in any effort the State undertakes to contest the request, subpoena or other legal process, at no additional cost to the State.
- 10.7 Contractor Confidential Information. Contractor shall clearly identify in writing all information it claims to be confidential or proprietary upon providing such information to the State. For the purposes of complying with its legal obligations, the State is under no obligation to accept the Contractor's designation of material as confidential. Contractor acknowledges that the State is subject to State and federal laws governing disclosure of information including, but not limited to, RSA Chapter 91-A. In the event the State receives a request for the information identified by Contractor as confidential, the State shall notify Contractor and specify the date the State will be releasing the requested information. At the request of the State, Contractor shall cooperate and

EXHIBIT A

assist the State with the collection and review of Contractor's information, at no additional expense to the State. Any effort to prohibit or enjoin the release of the information shall be Contractor's sole responsibility and at Contractor's sole expense. If Contractor fails to obtain a court order enjoining the disclosure, the State shall release the information on the date specified in the State's notice to Contractor, without any liability to the State.

10.8 This covenant in paragraph 10 shall survive the termination of this Contract.

1.7. Paragraph 12, Assignment/Delegation/Subcontracts, is amended by adding subparagraph 12.3 as follows:

12.3. Subcontractors are subject to the same contractual conditions as the Contractor and the Contractor is responsible to ensure subcontractor compliance with those conditions. The Contractor shall have written agreements with all subcontractors, specifying the work to be performed and how corrective action shall be managed if the subcontractor's performance is inadequate. The Contractor shall manage the subcontractor's performance on an ongoing basis and take corrective action as necessary. The Contractor shall annually provide the State with a list of all subcontractors provided for under this Agreement and notify the State of any inadequate subcontractor performance.

1.8. Paragraph 12, Assignment/Delegation/Subcontracts, is amended by adding subparagraph 12.4 as follows:

12.4. In the event that Contractor should change ownership for any reason whatsoever that results in a change of control of the Contractor, the State shall have the option of:

- a. continuing under the Agreement with Contractor, its successors or assigns for the full remaining Term of the Agreement or for such period of time as determined necessary by the State;
- b. immediately terminate the Agreement without liability to or further compensation owed to Contractor, its successors or assigns.

1.9. Paragraph 25 is added to read:

25. FORCE MAJEURE

25.1 Neither Contractor nor the State shall be responsible for delays or failures in performance resulting from events beyond the control of such Party and without fault or negligence of such Party. Such events shall include, but not be limited to, acts of God, strikes, lock outs, riots, and acts of War, epidemics, acts of Government, fire, power failures, nuclear accidents, earthquakes, and unusually severe weather.

EXHIBIT A

25.2 Except in the event of the foregoing, Force Majeure events shall not include the Contractor's inability to hire or provide personnel needed for the Contractor's performance under the Contract.

2. Revisions to Standard Exhibits

2.1. Exhibit enter, is amended as follows:

2.1.1. Paragraph X, is amended as follows:

Do Not Return

New Hampshire Department of Health and Human Services



EXHIBIT B

Scope of Services

To be drafted in accordance with the selected Vendor’s proposal, as negotiated with the Department through the procurement process.

Do Not Return

Contractor Initials _____

Vendor Name

Page 1 of 1

Date _____

Do Not Return

New Hampshire Department of Health and Human Services



EXHIBIT C

Payment Terms

To be drafted in accordance with the selected Vendor’s proposal, as negotiated with the Department through the procurement process.

VENDOR NAME

Exhibit C

Contractor Initials _____

Do Not Return

Page 1 of 1

Date _____

Rev. 01/08/19

Do Not Return

**New Hampshire Department of Health and Human Services
Exhibit D**



CERTIFICATION REGARDING DRUG-FREE WORKPLACE REQUIREMENTS

The Vendor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of Sections 5151-5160 of the Drug-Free Workplace Act of 1988 (Pub. L. 100-690, Title V, Subtitle D; 41 U.S.C. 701 et seq.), and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

ALTERNATIVE I - FOR GRANTEES OTHER THAN INDIVIDUALS

**US DEPARTMENT OF HEALTH AND HUMAN SERVICES - CONTRACTORS
US DEPARTMENT OF EDUCATION - CONTRACTORS
US DEPARTMENT OF AGRICULTURE - CONTRACTORS**

This certification is required by the regulations implementing Sections 5151-5160 of the Drug-Free Workplace Act of 1988 (Pub. L. 100-690, Title V, Subtitle D; 41 U.S.C. 701 et seq.). The January 31, 1989 regulations were amended and published as Part II of the May 25, 1990 Federal Register (pages 21681-21691), and require certification by grantees (and by inference, sub-grantees and sub-contractors), prior to award, that they will maintain a drug-free workplace. Section 3017.630(c) of the regulation provides that a grantee (and by inference, sub-grantees and sub-contractors) that is a State may elect to make one certification to the Department in each federal fiscal year in lieu of certificates for each grant during the federal fiscal year covered by the certification. The certificate set out below is a material representation of fact upon which reliance is placed when the agency awards the grant. False certification or violation of the certification shall be grounds for suspension of payments, suspension or termination of grants, or government wide suspension or debarment. Contractors using this form should send it to:

Commissioner
NH Department of Health and Human Services
129 Pleasant Street,
Concord, NH 03301-6505

1. The grantee certifies that it will or will continue to provide a drug-free workplace by:
 - 1.1. Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the grantee's workplace and specifying the actions that will be taken against employees for violation of such prohibition;
 - 1.2. Establishing an ongoing drug-free awareness program to inform employees about
 - 1.2.1. The dangers of drug abuse in the workplace;
 - 1.2.2. The grantee's policy of maintaining a drug-free workplace;
 - 1.2.3. Any available drug counseling, rehabilitation, and employee assistance programs; and
 - 1.2.4. The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;
 - 1.3. Making it a requirement that each employee to be engaged in the performance of the grant be given a copy of the statement required by paragraph (a);
 - 1.4. Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the grant, the employee will
 - 1.4.1. Abide by the terms of the statement; and
 - 1.4.2. Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction;
 - 1.5. Notifying the agency in writing, within ten calendar days after receiving notice under subparagraph 1.4.2 from an employee or otherwise receiving actual notice of such conviction. Employers of convicted employees must provide notice, including position title, to every grant officer on whose grant activity the convicted employee was working, unless the Federal agency

Do Not Return

Do Not Return

**New Hampshire Department of Health and Human Services
Exhibit D**



- has designated a central point for the receipt of such notices. Notice shall include the identification number(s) of each affected grant;
- 1.6. Taking one of the following actions, within 30 calendar days of receiving notice under subparagraph 1.4.2, with respect to any employee who is so convicted
 - 1.6.1. Taking appropriate personnel action against such an employee, up to and including termination, consistent with the requirements of the Rehabilitation Act of 1973, as amended; or
 - 1.6.2. Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency;
 - 1.7. Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs 1.1, 1.2, 1.3, 1.4, 1.5, and 1.6.
2. The grantee may insert in the space provided below the site(s) for the performance of work done in connection with the specific grant.

Place of Performance (street address, city, county, state, zip code) (list each location)

Check ☐ if there are workplaces on file that are not identified here.

Vendor Name:

Date

Name:
Title:

Do Not Return

Vendor Initials _____

Date _____

Do Not Return**New Hampshire Department of Health and Human Services
Exhibit E****CERTIFICATION REGARDING LOBBYING**

The Vendor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of Section 319 of Public Law 101-121, Government wide Guidance for New Restrictions on Lobbying, and 31 U.S.C. 1352, and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

US DEPARTMENT OF HEALTH AND HUMAN SERVICES - CONTRACTORS
 US DEPARTMENT OF EDUCATION - CONTRACTORS
 US DEPARTMENT OF AGRICULTURE - CONTRACTORS

Programs (indicate applicable program covered):

- *Temporary Assistance to Needy Families under Title IV-A
- *Child Support Enforcement Program under Title IV-D
- *Social Services Block Grant Program under Title XX
- *Medicaid Program under Title XIX
- *Community Services Block Grant under Title VI
- *Child Care Development Block Grant under Title IV

The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement (and by specific mention sub-grantee or sub-contractor).
2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement (and by specific mention sub-grantee or sub-contractor), the undersigned shall complete and submit Standard Form LLL, (Disclosure Form to Report Lobbying, in accordance with its instructions, attached and identified as Standard Exhibit E-I.)
3. The undersigned shall require that the language of this certification be included in the award document for sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all sub-recipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

Vendor Name: _____

Date

Name:
Title:

Do Not Return

Exhibit E – Certification Regarding Lobbying

Vendor Initials _____

Do Not Return**New Hampshire Department of Health and Human Services
Exhibit F**

**CERTIFICATION REGARDING DEBARMENT, SUSPENSION
AND OTHER RESPONSIBILITY MATTERS**

The Vendor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of Executive Office of the President, Executive Order 12549 and 45 CFR Part 76 regarding Debarment, Suspension, and Other Responsibility Matters, and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

INSTRUCTIONS FOR CERTIFICATION

1. By signing and submitting this proposal (contract), the prospective primary participant is providing the certification set out below.
2. The inability of a person to provide the certification required below will not necessarily result in denial of participation in this covered transaction. If necessary, the prospective participant shall submit an explanation of why it cannot provide the certification. The certification or explanation will be considered in connection with the NH Department of Health and Human Services' (DHHS) determination whether to enter into this transaction. However, failure of the prospective primary participant to furnish a certification or an explanation shall disqualify such person from participation in this transaction.
3. The certification in this clause is a material representation of fact upon which reliance was placed when DHHS determined to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, DHHS may terminate this transaction for cause or default.
4. The prospective primary participant shall provide immediate written notice to the DHHS agency to whom this proposal (contract) is submitted if at any time the prospective primary participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
5. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this clause, have the meanings set out in the Definitions and Coverage sections of the rules implementing Executive Order 12549: 45 CFR Part 76. See the attached definitions.
6. The prospective primary participant agrees by submitting this proposal (contract) that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by DHHS.
7. The prospective primary participant further agrees by submitting this proposal that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion - Lower Tier Covered Transactions," provided by DHHS, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
8. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not debarred, suspended, ineligible, or involuntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Nonprocurement List (of excluded parties).
9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and

Do Not Return

Do Not Return**New Hampshire Department of Health and Human Services
Exhibit F**

information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

10. Except for transactions authorized under paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal government, DHHS may terminate this transaction for cause or default.

PRIMARY COVERED TRANSACTIONS

11. The prospective primary participant certifies to the best of its knowledge and belief, that it and its principals:
- 11.1. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;
 - 11.2. have not within a three-year period preceding this proposal (contract) been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or a contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
 - 11.3. are not presently indicted for otherwise criminally or civilly charged by a governmental entity (Federal, State or local) with commission of any of the offenses enumerated in paragraph (I)(b) of this certification; and
 - 11.4. have not within a three-year period preceding this application/proposal had one or more public transactions (Federal, State or local) terminated for cause or default.
12. Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal (contract).

LOWER TIER COVERED TRANSACTIONS

13. By signing and submitting this lower tier proposal (contract), the prospective lower tier participant, as defined in 45 CFR Part 76, certifies to the best of its knowledge and belief that it and its principals:
- 13.1. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency.
 - 13.2. where the prospective lower tier participant is unable to certify to any of the above, such prospective participant shall attach an explanation to this proposal (contract).
14. The prospective lower tier participant further agrees by submitting this proposal (contract) that it will include this clause entitled "Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion - Lower Tier Covered Transactions," without modification in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

Vendor Name: _____

Date_____
Name:
Title:**Do Not Return**

Do Not Return

**New Hampshire Department of Health and Human Services
Exhibit G**



**CERTIFICATION OF COMPLIANCE WITH REQUIREMENTS PERTAINING TO
FEDERAL NONDISCRIMINATION, EQUAL TREATMENT OF FAITH-BASED ORGANIZATIONS AND
WHISTLEBLOWER PROTECTIONS**

The Vendor identified in Section 1.3 of the General Provisions agrees by signature of the Contractor's representative as identified in Sections 1.11 and 1.12 of the General Provisions, to execute the following certification:

Vendor will comply, and will require any subgrantees or subcontractors to comply, with any applicable federal nondiscrimination requirements, which may include:

- the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. Section 3789d) which prohibits recipients of federal funding under this statute from discriminating, either in employment practices or in the delivery of services or benefits, on the basis of race, color, religion, national origin, and sex. The Act requires certain recipients to produce an Equal Employment Opportunity Plan;
- the Juvenile Justice Delinquency Prevention Act of 2002 (42 U.S.C. Section 5672(b)) which adopts by reference, the civil rights obligations of the Safe Streets Act. Recipients of federal funding under this statute are prohibited from discriminating, either in employment practices or in the delivery of services or benefits, on the basis of race, color, religion, national origin, and sex. The Act includes Equal Employment Opportunity Plan requirements;
- the Civil Rights Act of 1964 (42 U.S.C. Section 2000d, which prohibits recipients of federal financial assistance from discriminating on the basis of race, color, or national origin in any program or activity);
- the Rehabilitation Act of 1973 (29 U.S.C. Section 794), which prohibits recipients of Federal financial assistance from discriminating on the basis of disability, in regard to employment and the delivery of services or benefits, in any program or activity;
- the Americans with Disabilities Act of 1990 (42 U.S.C. Sections 12131-34), which prohibits discrimination and ensures equal opportunity for persons with disabilities in employment, State and local government services, public accommodations, commercial facilities, and transportation;
- the Education Amendments of 1972 (20 U.S.C. Sections 1681, 1683, 1685-86), which prohibits discrimination on the basis of sex in federally assisted education programs;
- the Age Discrimination Act of 1975 (42 U.S.C. Sections 6106-07), which prohibits discrimination on the basis of age in programs or activities receiving Federal financial assistance. It does not include employment discrimination;
- 28 C.F.R. pt. 31 (U.S. Department of Justice Regulations – OJJDP Grant Programs); 28 C.F.R. pt. 42 (U.S. Department of Justice Regulations – Nondiscrimination; Equal Employment Opportunity; Policies and Procedures); Executive Order No. 13279 (equal protection of the laws for faith-based and community organizations); Executive Order No. 13559, which provide fundamental principles and policy-making criteria for partnerships with faith-based and neighborhood organizations;
- 28 C.F.R. pt. 38 (U.S. Department of Justice Regulations – Equal Treatment for Faith-Based Organizations); and Whistleblower protections 41 U.S.C. §4712 and The National Defense Authorization Act (NDAA) for Fiscal Year 2013 (Pub. L. 112-239, enacted January 2, 2013) the Pilot Program for Enhancement of Contract Employee Whistleblower Protections, which protects employees against reprisal for certain whistle blowing activities in connection with federal grants and contracts.

The certificate set out below is a material representation of fact upon which reliance is placed when the agency awards the grant. False certification or violation of the certification shall be grounds for suspension of payments, suspension or termination of grants, or government wide suspension or debarment.

Do Not Return

Exhibit G

Vendor Initials _____

Certification of Compliance with requirements pertaining to Federal Nondiscrimination, Equal Treatment of Faith-Based Organizations
and Whistleblower protections

6/27/14
Rev. 10/21/14

Page 1 of 2

Date _____

Do Not Return**New Hampshire Department of Health and Human Services
Exhibit G**

In the event a Federal or State court or Federal or State administrative agency makes a finding of discrimination after a due process hearing on the grounds of race, color, religion, national origin, or sex against a recipient of funds, the recipient will forward a copy of the finding to the Office for Civil Rights, to the applicable contracting agency or division within the Department of Health and Human Services, and to the Department of Health and Human Services Office of the Ombudsman.

The Vendor identified in Section 1.3 of the General Provisions agrees by signature of the Contractor's representative as identified in Sections 1.11 and 1.12 of the General Provisions, to execute the following certification:

1. By signing and submitting this proposal (contract) the Vendor agrees to comply with the provisions indicated above.

Vendor Name: _____

Date _____

Name: _____
Title: _____**Do Not Return**

Exhibit G

Vendor Initials _____

Certification of Compliance with requirements pertaining to Federal Nondiscrimination, Equal Treatment of Faith-Based Organizations
and Whistleblower protections

6/27/14
Rev. 10/21/14

Page 2 of 2

Date _____

Do Not Return

**New Hampshire Department of Health and Human Services
Exhibit H**



CERTIFICATION REGARDING ENVIRONMENTAL TOBACCO SMOKE

Public Law 103-227, Part C - Environmental Tobacco Smoke, also known as the Pro-Children Act of 1994 (Act), requires that smoking not be permitted in any portion of any indoor facility owned or leased or contracted for by an entity and used routinely or regularly for the provision of health, day care, education, or library services to children under the age of 18, if the services are funded by Federal programs either directly or through State or local governments, by Federal grant, contract, loan, or loan guarantee. The law does not apply to children's services provided in private residences, facilities funded solely by Medicare or Medicaid funds, and portions of facilities used for inpatient drug or alcohol treatment. Failure to comply with the provisions of the law may result in the imposition of a civil monetary penalty of up to \$1000 per day and/or the imposition of an administrative compliance order on the responsible entity.

The Vendor identified in Section 1.3 of the General Provisions agrees, by signature of the Contractor's representative as identified in Section 1.11 and 1.12 of the General Provisions, to execute the following certification:

1. By signing and submitting this contract, the Vendor agrees to make reasonable efforts to comply with all applicable provisions of Public Law 103-227, Part C, known as the Pro-Children Act of 1994.

Vendor Name:

Date

Name:
Title:

Do Not Return

Vendor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services



Exhibit I

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT **BUSINESS ASSOCIATE AGREEMENT**

The Contractor identified in Section 1.3 of the General Provisions of the Agreement agrees to comply with the Health Insurance Portability and Accountability Act, Public Law 104-191 and with the Standards for Privacy and Security of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 applicable to business associates. As defined herein, "Business Associate" shall mean the Contractor and subcontractors and agents of the Contractor that receive, use or have access to protected health information under this Agreement and "Covered Entity" shall mean the State of New Hampshire, Department of Health and Human Services.

(1) Definitions.

- a. "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
- b. "Business Associate" has the meaning given such term in section 160.103 of Title 45, Code of Federal Regulations.
- c. "Covered Entity" has the meaning given such term in section 160.103 of Title 45, Code of Federal Regulations.
- d. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 CFR Section 164.501.
- e. "Data Aggregation" shall have the same meaning as the term "data aggregation" in 45 CFR Section 164.501.
- f. "Health Care Operations" shall have the same meaning as the term "health care operations" in 45 CFR Section 164.501.
- g. "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, Title XIII, Subtitle D, Part 1 & 2 of the American Recovery and Reinvestment Act of 2009.
- h. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and the Standards for Privacy and Security of Individually Identifiable Health Information, 45 CFR Parts 160, 162 and 164 and amendments thereto.
- i. "Individual" shall have the same meaning as the term "individual" in 45 CFR Section 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.501(g).
- j. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
- k. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR Section 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

Do Not Return
3/2014

Exhibit I
Health Insurance Portability Act
Business Associate Agreement
Page 1 of 6

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services



Exhibit I

- l. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR Section 164.103.
- m. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.
- n. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 164, Subpart C, and amendments thereto.
- o. "Unsecured Protected Health Information" means protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.
- p. Other Definitions - All terms not otherwise defined herein shall have the meaning established under 45 C.F.R. Parts 160, 162 and 164, as amended from time to time, and the HITECH Act.

(2) **Business Associate Use and Disclosure of Protected Health Information.**

- a. Business Associate shall not use, disclose, maintain or transmit Protected Health Information (PHI) except as reasonably necessary to provide the services outlined under Exhibit A of the Agreement. Further, Business Associate, including but not limited to all its directors, officers, employees and agents, shall not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
- b. Business Associate may use or disclose PHI:
 - I. For the proper management and administration of the Business Associate;
 - II. As required by law, pursuant to the terms set forth in paragraph d. below; or
 - III. For data aggregation purposes for the health care operations of Covered Entity.
- c. To the extent Business Associate is permitted under the Agreement to disclose PHI to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable assurances from the third party that such PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party; and (ii) an agreement from such third party to notify Business Associate, in accordance with the HIPAA Privacy, Security, and Breach Notification Rules of any breaches of the confidentiality of the PHI, to the extent it has obtained knowledge of such breach.
- d. The Business Associate shall not, unless such disclosure is reasonably necessary to provide services under Exhibit A of the Agreement, disclose any PHI in response to a request for disclosure on the basis that it is required by law, without first notifying Covered Entity so that Covered Entity has an opportunity to object to the disclosure and to seek appropriate relief. If Covered Entity objects to such disclosure, the Business

Do Not Return
3/2014

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services



Exhibit I

Associate shall refrain from disclosing the PHI until Covered Entity has exhausted all remedies.

- e. If the Covered Entity notifies the Business Associate that Covered Entity has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Business Associate shall be bound by such additional restrictions and shall not disclose PHI in violation of such additional restrictions and shall abide by any additional security safeguards.

(3) Obligations and Activities of Business Associate.

- a. The Business Associate shall notify the Covered Entity's Privacy Officer immediately after the Business Associate becomes aware of any use or disclosure of protected health information not provided for by the Agreement including breaches of unsecured protected health information and/or any security incident that may have an impact on the protected health information of the Covered Entity.
- b. The Business Associate shall immediately perform a risk assessment when it becomes aware of any of the above situations. The risk assessment shall include, but not be limited to:
- o The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
 - o The unauthorized person used the protected health information or to whom the disclosure was made;
 - o Whether the protected health information was actually acquired or viewed
 - o The extent to which the risk to the protected health information has been mitigated.

The Business Associate shall complete the risk assessment within 48 hours of the breach and immediately report the findings of the risk assessment in writing to the Covered Entity.

- c. The Business Associate shall comply with all sections of the Privacy, Security, and Breach Notification Rule.
- d. Business Associate shall make available all of its internal policies and procedures, books and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of Covered Entity to the Secretary for purposes of determining Covered Entity's compliance with HIPAA and the Privacy and Security Rule.
- e. Business Associate shall require all of its business associates that receive, use or have access to PHI under the Agreement, to agree in writing to adhere to the same restrictions and conditions on the use and disclosure of PHI contained herein, including the duty to return or destroy the PHI as provided under Section 3 (I). The Covered Entity shall be considered a direct third party beneficiary of the Contractor's business associate agreements with Contractor's intended business associates, who will be receiving PHI

Do Not Return
3/2014

Exhibit I
Health Insurance Portability Act
Business Associate Agreement
Page 3 of 6

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services



Exhibit I

pursuant to this Agreement, with rights of enforcement and indemnification from such business associates who shall be governed by standard Paragraph #13 of the standard contract provisions (P-37) of this Agreement for the purpose of use and disclosure of protected health information.

- f. Within five (5) business days of receipt of a written request from Covered Entity, Business Associate shall make available during normal business hours at its offices all records, books, agreements, policies and procedures relating to the use and disclosure of PHI to the Covered Entity, for purposes of enabling Covered Entity to determine Business Associate's compliance with the terms of the Agreement.
- g. Within ten (10) business days of receiving a written request from Covered Entity, Business Associate shall provide access to PHI in a Designated Record Set to the Covered Entity, or as directed by Covered Entity, to an individual in order to meet the requirements under 45 CFR Section 164.524.
- h. Within ten (10) business days of receiving a written request from Covered Entity for an amendment of PHI or a record about an individual contained in a Designated Record Set, the Business Associate shall make such PHI available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under 45 CFR Section 164.526.
- i. Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.
- j. Within ten (10) business days of receiving a written request from Covered Entity for a request for an accounting of disclosures of PHI, Business Associate shall make available to Covered Entity such information as Covered Entity may require to fulfill its obligations to provide an accounting of disclosures with respect to PHI in accordance with 45 CFR Section 164.528.
- k. In the event any individual requests access to, amendment of, or accounting of PHI directly from the Business Associate, the Business Associate shall within two (2) business days forward such request to Covered Entity. Covered Entity shall have the responsibility of responding to forwarded requests. However, if forwarding the individual's request to Covered Entity would cause Covered Entity or the Business Associate to violate HIPAA and the Privacy and Security Rule, the Business Associate shall instead respond to the individual's request as required by such law and notify Covered Entity of such response as soon as practicable.
- l. Within ten (10) business days of termination of the Agreement, for any reason, the Business Associate shall return or destroy, as specified by Covered Entity, all PHI received from, or created or received by the Business Associate in connection with the Agreement, and shall not retain any copies or back-up tapes of such PHI. If return or destruction is not feasible, or the disposition of the PHI has been otherwise agreed to in the Agreement, Business Associate shall continue to extend the protections of the Agreement, to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business

Do Not Return
3/2014

Exhibit I
Health Insurance Portability Act
Business Associate Agreement
Page 4 of 6

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services



Exhibit I

Associate maintains such PHI. If Covered Entity, in its sole discretion, requires that the Business Associate destroy any or all PHI, the Business Associate shall certify to Covered Entity that the PHI has been destroyed.

(4) Obligations of Covered Entity

- a. Covered Entity shall notify Business Associate of any changes or limitation(s) in its Notice of Privacy Practices provided to individuals in accordance with 45 CFR Section 164.520, to the extent that such change or limitation may affect Business Associate's use or disclosure of PHI.
- b. Covered Entity shall promptly notify Business Associate of any changes in, or revocation of permission provided to Covered Entity by individuals whose PHI may be used or disclosed by Business Associate under this Agreement, pursuant to 45 CFR Section 164.506 or 45 CFR Section 164.508.
- c. Covered entity shall promptly notify Business Associate of any restrictions on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(5) Termination for Cause

In addition to Paragraph 10 of the standard terms and conditions (P-37) of this Agreement the Covered Entity may immediately terminate the Agreement upon Covered Entity's knowledge of a breach by Business Associate of the Business Associate Agreement set forth herein as Exhibit I. The Covered Entity may either immediately terminate the Agreement or provide an opportunity for Business Associate to cure the alleged breach within a timeframe specified by Covered Entity. If Covered Entity determines that neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(6) Miscellaneous

- a. Definitions and Regulatory References. All terms used, but not otherwise defined herein, shall have the same meaning as those terms in the Privacy and Security Rule, amended from time to time. A reference in the Agreement, as amended to include this Exhibit I, to a Section in the Privacy and Security Rule means the Section as in effect or as amended.
- b. Amendment. Covered Entity and Business Associate agree to take such action as is necessary to amend the Agreement, from time to time as is necessary for Covered Entity to comply with the changes in the requirements of HIPAA, the Privacy and Security Rule, and applicable federal and state law.
- c. Data Ownership. The Business Associate acknowledges that it has no ownership rights with respect to the PHI provided by or created on behalf of Covered Entity.
- d. Interpretation. The parties agree that any ambiguity in the Agreement shall be resolved to permit Covered Entity to comply with HIPAA, the Privacy and Security Rule.

Do Not Return
3/2014

Exhibit I
Health Insurance Portability Act
Business Associate Agreement
Page 5 of 6

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services



Exhibit I

- e. Segregation. If any term or condition of this Exhibit I or the application thereof to any person(s) or circumstance is held invalid, such invalidity shall not affect other terms or conditions which can be given effect without the invalid term or condition; to this end the terms and conditions of this Exhibit I are declared severable.
- f. Survival. Provisions in this Exhibit I regarding the use and disclosure of PHI, return or destruction of PHI, extensions of the protections of the Agreement in section (3) I, the defense and indemnification provisions of section (3) e and Paragraph 13 of the standard terms and conditions (P-37), shall survive the termination of the Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Exhibit I.

Department of Health and Human Services

The State

Name of the Contractor

Signature of Authorized Representative

Signature of Authorized Representative

Name of Authorized Representative

Name of Authorized Representative

Title of Authorized Representative

Title of Authorized Representative

Date

Date

Do Not Return
3/2014

Exhibit I
Health Insurance Portability Act
Business Associate Agreement
Page 6 of 6

Contractor Initials _____

Date _____

Do Not Return

**New Hampshire Department of Health and Human Services
Exhibit J**



**CERTIFICATION REGARDING THE FEDERAL FUNDING ACCOUNTABILITY AND TRANSPARENCY
ACT (FFATA) COMPLIANCE**

The Federal Funding Accountability and Transparency Act (FFATA) requires prime awardees of individual Federal grants equal to or greater than \$25,000 and awarded on or after October 1, 2010, to report on data related to executive compensation and associated first-tier sub-grants of \$25,000 or more. If the initial award is below \$25,000 but subsequent grant modifications result in a total award equal to or over \$25,000, the award is subject to the FFATA reporting requirements, as of the date of the award.

In accordance with 2 CFR Part 170 (Reporting Subaward and Executive Compensation Information), the Department of Health and Human Services (DHHS) must report the following information for any subaward or contract award subject to the FFATA reporting requirements:

1. Name of entity
2. Amount of award
3. Funding agency
4. NAICS code for contracts / CFDA program number for grants
5. Program source
6. Award title descriptive of the purpose of the funding action
7. Location of the entity
8. Principle place of performance
9. Unique identifier of the entity (DUNS #)
10. Total compensation and names of the top five executives if:
 - 10.1. More than 80% of annual gross revenues are from the Federal government, and those revenues are greater than \$25M annually and
 - 10.2. Compensation information is not already available through reporting to the SEC.

Prime grant recipients must submit FFATA required data by the end of the month, plus 30 days, in which the award or award amendment is made.

The Contractor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of The Federal Funding Accountability and Transparency Act, Public Law 109-282 and Public Law 110-252, and 2 CFR Part 170 (Reporting Subaward and Executive Compensation Information), and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

The below named Contractor agrees to provide needed information as outlined above to the NH Department of Health and Human Services and to comply with all applicable provisions of the Federal Financial Accountability and Transparency Act.

Contractor Name: _____

Date

Name:
Title:

Do Not Return

Do Not Return

**New Hampshire Department of Health and Human Services
Exhibit J**



FORM A

As the Contractor identified in Section 1.3 of the General Provisions, I certify that the responses to the below listed questions are true and accurate.

1. The DUNS number for your entity is: _____
2. In your business or organization's preceding completed fiscal year, did your business or organization receive (1) 80 percent or more of your annual gross revenue in U.S. federal contracts, subcontracts, loans, grants, sub-grants, and/or cooperative agreements; and (2) \$25,000,000 or more in annual gross revenues from U.S. federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements?

_____ NO _____ YES

If the answer to #2 above is NO, stop here

If the answer to #2 above is YES, please answer the following:

3. Does the public have access to information about the compensation of the executives in your business or organization through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C.78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986?

_____ NO _____ YES

If the answer to #3 above is YES, stop here

If the answer to #3 above is NO, please answer the following:

4. The names and compensation of the five most highly compensated officers in your business or organization are as follows:

Name: _____	Amount: _____
Name: _____	Amount: _____
Name: _____	Amount: _____
Name: _____	Amount: _____
Name: _____	Amount: _____

Do Not Return

Do Not Return

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



A. Definitions

The following terms may be reflected and have the described meaning in this document:

1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
2. "Computer Security Incident" shall have the same meaning "Computer Security Incident" in section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce.
3. "Confidential Information" or "Confidential Data" means all confidential information disclosed by one party to the other such as all medical, health, financial, public assistance benefits and personal information including without limitation, Substance Abuse Treatment Records, Case Records, Protected Health Information and Personally Identifiable Information.

Confidential Information also includes any and all information owned or managed by the State of NH - created, received from or on behalf of the Department of Health and Human Services (DHHS) or accessed in the course of performing contracted services - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personal Information (PI), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and confidential information.

4. "End User" means any person or entity (e.g., contractor, contractor's employee, business associate, subcontractor, other downstream user, etc.) that receives DHHS data or derivative data in accordance with the terms of this Contract.
5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.
6. "Incident" means an act that potentially violates an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic

Do Not Return

V5. Last update 10/09/18

Exhibit K
DHHS Information
Security Requirements
Page 1 of 9

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services**Exhibit K****DHHS Information Security Requirements**

mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

7. "Open Wireless Network" means any network or segment of a network that is not designated by the State of New Hampshire's Department of Information Technology or delegate as a protected network (designed, tested, and approved, by means of the State, to transmit) will be considered an open network and not adequately secure for the transmission of unencrypted PI, PFI, PHI or confidential DHHS data.
8. "Personal Information" (or "PI") means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, personal information as defined in New Hampshire RSA 359-C:19, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
9. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
10. "Protected Health Information" (or "PHI") has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 C.F.R. § 160.103.
11. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C, and amendments thereto.
12. "Unsecured Protected Health Information" means Protected Health Information that is not secured by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

I. RESPONSIBILITIES OF DHHS AND THE CONTRACTOR**A. Business Use and Disclosure of Confidential Information.**

1. The Contractor must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Contract. Further, Contractor, including but not limited to all its directors, officers, employees and agents, must not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
2. The Contractor must not disclose any Confidential Information in response to a

Do Not Return

V5. Last update 10/09/18

Exhibit K
DHHS Information
Security Requirements
Page 2 of 9

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



request for disclosure on the basis that it is required by law, in response to a subpoena, etc., without first notifying DHHS so that DHHS has an opportunity to consent or object to the disclosure.

3. If DHHS notifies the Contractor that DHHS has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Contractor must be bound by such additional restrictions and must not disclose PHI in violation of such additional restrictions and must abide by any additional security safeguards.
4. The Contractor agrees that DHHS Data or derivative there from disclosed to an End User must only be used pursuant to the terms of this Contract.
5. The Contractor agrees DHHS Data obtained under this Contract may not be used for any other purposes that are not indicated in this Contract.
6. The Contractor agrees to grant access to the data to the authorized representatives of DHHS for the purpose of inspecting to confirm compliance with the terms of this Contract.

II. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If End User is transmitting DHHS data containing Confidential Data between applications, the Contractor attests the applications have been evaluated by an expert knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.
2. Computer Disks and Portable Storage Devices. End User may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting DHHS data.
3. Encrypted Email. End User may only employ email to transmit Confidential Data if email is encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
4. Encrypted Web Site. If End User is employing the Web to transmit Confidential Data, the secure socket layers (SSL) must be used and the web site must be secure. SSL encrypts data transmitted via a Web site.
5. File Hosting Services, also known as File Sharing Sites. End User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. End User may only transmit Confidential Data via *certified* ground mail within the continental U.S. and when sent to a named individual.
7. Laptops and PDA. If End User is employing portable devices to transmit Confidential Data said devices must be encrypted and password-protected.
8. Open Wireless Networks. End User may not transmit Confidential Data via an open

Do Not Return

V5. Last update 10/09/18

Exhibit K
DHHS Information
Security Requirements
Page 3 of 9

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



wireless network. End User must employ a virtual private network (VPN) when remotely transmitting via an open wireless network.

9. Remote User Communication. If End User is employing remote communication to access or transmit Confidential Data, a virtual private network (VPN) must be installed on the End User's mobile device(s) or laptop from which information will be transmitted or accessed.
10. SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. If End User is employing an SFTP to transmit Confidential Data, End User will structure the Folder and access privileges to prevent inappropriate disclosure of information. SFTP folders and sub-folders used for transmitting Confidential Data will be coded for 24-hour auto-deletion cycle (i.e. Confidential Data will be deleted every 24 hours).
11. Wireless Devices. If End User is transmitting Confidential Data via wireless devices, all data must be encrypted to prevent inappropriate disclosure of information.

III. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The Contractor will only retain the data and any derivative of the data for the duration of this Contract. After such time, the Contractor will have 30 days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Contract. To this end, the parties must:

A. Retention

1. The Contractor agrees it will not store, transfer or process data collected in connection with the services rendered under this Contract outside of the United States. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data and Disaster Recovery locations.
2. The Contractor agrees to ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
3. The Contractor agrees to provide security awareness and education for its End Users in support of protecting Department confidential information.
4. The Contractor agrees to retain all electronic and hard copies of Confidential Data in a secure location and identified in section IV. A.2
5. The Contractor agrees Confidential Data stored in a Cloud must be in a FedRAMP/HITECH compliant solution and comply with all applicable statutes and regulations regarding the privacy and security. All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a

Do Not Return

V5. Last update 10/09/18

Exhibit K
DHHS Information
Security Requirements
Page 4 of 9

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services**Exhibit K****DHHS Information Security Requirements**

whole, must have aggressive intrusion-detection and firewall protection.

6. The Contractor agrees to and ensures its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.

B. Disposition

1. If the Contractor will maintain any Confidential Information on its systems (or its sub-contractor systems), the Contractor will maintain a documented process for securely disposing of such data upon request or contract termination; and will obtain written certification for any State of New Hampshire data destroyed by the Contractor or any subcontractors as a part of ongoing, emergency, and or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion and media sanitization, or otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce. The Contractor will document and certify in writing at time of the data destruction, and will provide written certification to the Department upon request. The written certification will include all details necessary to demonstrate data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and Contractor prior to destruction.
2. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to destroy all hard copies of Confidential Data using a secure method such as shredding.
3. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.

IV. PROCEDURES FOR SECURITY

- A. Contractor agrees to safeguard the DHHS Data received under this Contract, and any derivative data or files, as follows:
 1. The Contractor will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services.
 2. The Contractor will maintain policies and procedures to protect Department confidential information throughout the information lifecycle, where applicable, (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

Do Not Return

V5. Last update 10/09/18

Exhibit K
DHHS Information
Security Requirements
Page 5 of 9

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services**Exhibit K****DHHS Information Security Requirements**

3. The Contractor will maintain appropriate authentication and access controls to contractor systems that collect, transmit, or store Department confidential information where applicable.
4. The Contractor will ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
5. The Contractor will provide regular security awareness and education for its End Users in support of protecting Department confidential information.
6. If the Contractor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the Contractor will maintain a program of an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that at a minimum match those for the Contractor, including breach notification requirements.
7. The Contractor will work with the Department to sign and comply with all applicable State of New Hampshire and Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s). Agreements will be completed and signed by the Contractor and any applicable sub-contractors prior to system access being authorized.
8. If the Department determines the Contractor is a Business Associate pursuant to 45 CFR 160.103, the Contractor will execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.
9. The Contractor will work with the Department at its request to complete a System Management Survey. The purpose of the survey is to enable the Department and Contractor to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the Contractor engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the Contractor, or the Department may request the survey be completed when the scope of the engagement between the Department and the Contractor changes.
10. The Contractor will not store, knowingly or unknowingly, any State of New Hampshire or Department data offshore or outside the boundaries of the United States unless prior express written consent is obtained from the Information Security Office leadership member within the Department.
11. Data Security Breach Liability. In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the breach. The State shall recover from the Contractor all costs of response and recovery from

Do Not Return

V5. Last update 10/09/18

Exhibit K
DHHS Information
Security Requirements
Page 6 of 9

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



the breach, including but not limited to: credit monitoring services, mailing costs and costs associated with website and telephone call center services necessary due to the breach.

12. Contractor must, comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable health information and as applicable under State law.
13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology. Refer to Vendor Resources/Procurement at <https://www.nh.gov/doit/vendor/index.htm> for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors.
14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor will notify the State's Privacy Officer and the State's Security Officer of any security breach immediately, at the email addresses provided in Section VI. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.
15. Contractor must restrict access to the Confidential Data obtained under this Contract to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Contract.
16. The Contractor must ensure that all End Users:
 - a. comply with such safeguards as referenced in Section IV A. above, implemented to protect Confidential Information that is furnished by DHHS under this Contract from loss, theft or inadvertent disclosure.
 - b. safeguard this information at all times.
 - c. ensure that laptops and other electronic devices/media containing PHI, PI, or PFI are encrypted and password-protected.
 - d. send emails containing Confidential Information only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.

Do Not Return

V5. Last update 10/09/18

Exhibit K
DHHS Information
Security Requirements
Page 7 of 9

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



- e. limit disclosure of the Confidential Information to the extent permitted by law.
- f. Confidential Information received under this Contract and individually identifiable data derived from DHHS Data, must be stored in an area that is physically and technologically secure from access by unauthorized persons during duty hours as well as non-duty hours (e.g., door locks, card keys, biometric identifiers, etc.).
- g. only authorized End Users may transmit the Confidential Data, including any derivative files containing personally identifiable information, and in all cases, such data must be encrypted at all times when in transit, at rest, or when stored on portable media as required in section IV above.
- h. in all other instances Confidential Data must be maintained, used and disclosed using appropriate safeguards, as determined by a risk-based assessment of the circumstances involved.
- i. understand that their user credentials (user name and password) must not be shared with anyone. End Users will keep their credential information secure. This applies to credentials used to access the site directly or indirectly through a third party application.

Contractor is responsible for oversight and compliance of their End Users. DHHS reserves the right to conduct onsite inspections to monitor compliance with this Contract, including the privacy and security requirements provided in herein, HIPAA, and other applicable laws and Federal regulations until such time the Confidential Data is disposed of in accordance with this Contract.

V. LOSS REPORTING

The Contractor must notify the State's Privacy Officer and Security Officer of any Security Incidents and Breaches immediately, at the email addresses provided in Section VI.

The Contractor must further handle and report Incidents and Breaches involving PHI in accordance with the agency's documented Incident Handling and Breach Notification procedures and in accordance with 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, Contractor's compliance with all applicable obligations and procedures, Contractor's procedures must also address how the Contractor will:

1. Identify Incidents;
2. Determine if personally identifiable information is involved in Incidents;
3. Report suspected or confirmed Incidents as required in this Exhibit or P-37;
4. Identify and convene a core response group to determine the risk level of Incidents and determine risk-based responses to Incidents; and

Do Not Return

V5. Last update 10/09/18

Exhibit K
DHHS Information
Security Requirements
Page 8 of 9

Contractor Initials _____

Date _____

Do Not Return

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



5. Determine whether Breach notification is required, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures.

Incidents and/or Breaches that implicate PI must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

VI. PERSONS TO CONTACT

A. DHHS Privacy Officer:

DHHSPrivacyOfficer@dhhs.nh.gov

B. DHHS Security Officer:

DHHSInformationSecurityOffice@dhhs.nh.gov

Do Not Return

V5. Last update 10/09/18

Contractor Initials _____

Date _____

Appendix B Contract Monitoring Provisions

Management Questionnaire

All Vendors responding to Department-issued Requests for Proposals (RFPs), Requests for Bids (RFBs), or Requests for Applications (RFAs) must complete and return this Management Questionnaire.

	Question	YES	NO	N/A
1.	Was your organization established more than two years ago?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2.	During the past 18 months, have you experienced staff turnover in positions that will be involved in the administration of the contract?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3.	Have you managed the same or a similar contract or program during one of the last five (5) calendar years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.	Have you received federal funds from the Department through a contract during one of the last five (5) calendar years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5.	Were you ever provided formal written notification from the Department that you were in non-compliance or failed to perform in accordance with contract provisions or requirements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.	If you had a Single Audit performed in accordance with the Federal Uniform Guidance (2 CFR 200 subpart F (200.500)) by an external entity or an audit performed by a state or federal agency during the most recently completed fiscal year, did the audit include any findings?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7.	Have you ever been required to return payments to the Department as a result of an audit, unallowable expenditure or any other reason?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8.	Has your organization implemented a new accounting, financial, or programmatic IT system within the last two years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
9.	Are you aware of any ongoing or pending lawsuits filed against your organization or any investigations or inspections of your organization by any state or federal regulatory agency within the last two years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
10.	With Department approval, if you intend to subcontract a portion of the work under the resulting contract to another entity, do you have competitive bid procedures for purchases and personal services contracts compliant with state and federal regulations, laws, and rules?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
11.	With Department approval, if you intend to subcontract a portion of the work under the resulting contract to another entity, do you have written policies and procedures for subrecipient/contractor determinations, risk assessments, and subrecipient monitoring as required under Federal Uniform Guidance (2 CFR subpart D (200.300))?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Appendix B Contract Monitoring Provisions

12.	Does your accounting system identify the receipt and expenditure of program funds separately by each contract or grant, and by line item categories?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
13.	Does your organization maintain a formal system of segregation of duties for procurement, time keeping, and bank statement reconciliation activities?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
14.	Do you have procedures to ensure expenditures are reviewed by an independent person* to determine that all expenditures are allowable under the terms of the contract as well as federal and state regulations, laws and rules?*	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
15.	Are time distribution records maintained for each employee performing contracted services that account for time spent working on the contract versus time spent on all other activities?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
16.	Does your financial system compare amounts spent to date with budgeted amounts for each award?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
17.	Does your accounting or financial system include budgetary controls to prevent incurring obligations in excess of total funds available for a grant or a cost category (e.g., personnel costs, equipment, travel)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
18.	Do you maintain written policy and procedures for all aspects of financial transactions and accounting related to time keeping, a record retention, procurement, and asset management that are compliant with Federal Uniform Guidance requirements (2 CFR subpart D (200.300))?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

*An independent person can be any individual within an organization or an outside third party, who verifies that an expenditure made by another person, is appropriate and in accordance with the terms of the contract. For example, one person would be responsible for making a purchase or authorizing payment and a second independent person verifies that funds were spent appropriately. If you do not have an independent person, please mark "No" for Question 14.

Marking No or N/A for any question on the Management Questionnaire does not preclude a Vendor from being selected.

I hereby declare that the answers provided in this Management Questionnaire are accurate and true to the best of my knowledge.

Signature

Printed Name & Job Title

Date

APPENDIX C

Addendum to CLAS Section of RFP for Purpose of Documenting Title VI Compliance

All DHHS applicants are required to complete the following two (2) steps as part of their application:

- (1) Perform an individualized organizational assessment, using the four-factor analysis, to determine the extent of language assistance to provide for programs, services and/or activities; and;
- (2) Taking into account the outcome of the four-factor analysis, respond to the questions below.

Background:

Title VI of the Civil Rights Act of 1964 and its implementing regulations provide that no person shall be subjected to discrimination on the basis of race, color, or national origin under any program that receives Federal financial assistance. The courts have held that national origin discrimination includes discrimination on the basis of limited English proficiency. Any organization or individual that receives Federal financial assistance, through either a grant, contract, or subcontract is a covered entity under Title VI. Examples of covered entities include the NH Department of Health and Human Services and its contractors.

Covered entities are required to take reasonable steps to ensure **meaningful access** by persons with limited English proficiency (LEP) to their programs and activities. LEP persons are those with a limited ability to speak, read, write or understand English.

The **key** to ensuring meaningful access by LEP persons is effective communication. An agency or provider can ensure effective communication by developing and implementing a language assistance program that includes policies and procedures for identifying and assessing the language needs of its LEP clients/applicants, and that provides for an array of language assistance options, notice to LEP persons of the right to receive language assistance free of charge, training of staff, periodic monitoring of the program, and translation of certain written materials.

The Office for Civil Rights (OCR) is the federal agency responsible for enforcing Title VI. OCR recognizes that covered entities vary in size, the number of LEP clients needing assistance, and the nature of the services provided. Accordingly, covered entities have some flexibility in how they address the needs of their LEP clients. (In other words, it is understood that one size language assistance program does not fit all covered entities.)

The **starting point** for covered entities to determine the extent of their obligation to provide LEP services is to apply a four-factor analysis to their organization. It is important to understand that the flexibility afforded in addressing the needs of LEP clients **does not diminish** the obligation covered entities have to address those needs.

APPENDIX C

Examples of practices that may violate Title VI include:

- Limiting participation in a program or activity due to a person's limited English proficiency;
- Providing services to LEP persons that are more limited in scope or are lower in quality than those provided to other persons (such as when there is no qualified interpretation provided);
- Failing to inform LEP persons of the right to receive free interpreter services and/or requiring LEP persons to provide their own interpreter;
- Subjecting LEP persons to unreasonable delays in the delivery of services.

Applicant STEP #1 – Individualized Assessment Using Four-Factor Analysis

The four-factor analysis helps an organization determine the right mix of services to provide to their LEP clients. The right mix of services is based upon an individualized assessment, involving the balancing of the following four factors.

- (1) The **number** or proportion of LEP persons served or likely to be encountered in the population that is eligible for the program;
- (2) The **frequency** with which LEP individuals come in contact with the program, activity or service;
- (3) The **importance** or impact of the contact upon the lives of the person(s) served by the program, activity or service;
- (4) The **resources** available to the organization to provide effective language assistance.

This addendum was created to facilitate an applicant's application of the four-factor analysis to the services they provide. At this stage, applicants are not required to submit their four-factor analysis as part of their application. **However, successful applicants will be required to submit a detailed description of the language assistance services they will provide to LEP persons to ensure meaningful access to their programs and/or services, within 10 days of the date the contract is approved by Governor and Council.** For further guidance, please see the Bidder's Reference for Completing the Culturally and Linguistically Appropriate Services (CLAS) Section of the RFP, which is available in the Vendor/RFP Section of the DHHS website.

APPENDIX C

Important Items to Consider When Evaluating the Four Factors.

Factor #1 The number or proportion of LEP persons served or encountered in the population that is eligible for the program.

Considerations:

- The eligible population is specific to the program, activity or service. It includes LEP persons serviced by the program, as well as those directly affected by the program, activity or service.
- Organizations are required not only to examine data on LEP persons served by their program, but also those in the community who are **eligible** for the program (but who are not currently served or participating in the program due to existing language barriers).
- Relevant data sources may include information collected by program staff, as well as external data, such as the latest Census Reports.
- Recipients are required to apply this analysis to each language in the service area. When considering the number or proportion of LEP individuals in a service area, recipients should consider whether the minor children their programs serve have LEP parent(s) or guardian(s) with whom the recipient may need to interact. It is also important to consider language minority populations that are eligible for the programs or services, but are not currently served or participating in the program, due to existing language barriers.
- An effective means of determining the number of LEP persons served is to record the preferred languages of people who have day-to-day contact with the program.
- It is important to remember that the **focus** of the analysis is on the lack of English proficiency, not the ability to speak more than one language.

Factor #2: The frequency with which LEP individuals come in contact with the program, activity or service.

- The more frequently a recipient entity has contact with individuals in a particular language group, the more likely that language assistance in that language is needed. For example, the steps that are reasonable for a recipient that serves an LEP person on a one-time basis will be very different from those that are expected from a recipient that serves LEP persons daily.
- Even recipients that serve people from a particular language group infrequently or on an unpredictable basis should use this four-factor analysis to determine what to do if an LEP person seeks services from their program.
- The resulting plan may be as simple as being prepared to use a telephone interpreter service.
- The key is to have a plan in place.

APPENDIX C

Factor #3 The importance or impact of the contact upon the lives of the person(s) served by the program, activity or service.
<ul style="list-style-type: none">• The more important a recipient's activity, program or service, or the greater the possible consequence of the contact to the LEP persons, the more likely language services are needed.• When considering this factor, the recipient should determine both the importance, as well as the urgency of the service. For example, if the communication is both important and urgent (such as the need to communicate information about an emergency medical procedure), it is more likely that immediate language services are required. If the information to be communicated is important but not urgent (such as the need to communicate information about elective surgery, where delay will not have any adverse impact on the patient's health), it is likely that language services are required, but that such services can be delayed for a reasonable length of time.
Factor #4 The resources available to the organization to provide effective language assistance.
<ul style="list-style-type: none">• A recipient's level of resources and the costs of providing language assistance services is another factor to consider in the analysis.• Remember, however, that cost is merely one factor in the analysis. Level of resources and costs do not diminish the requirement to address the need, however they may be considered in determining how the need is addressed;• Resources and cost issues can often be reduced, for example, by sharing language assistance materials and services among recipients. Therefore, recipients should carefully explore the most cost-effective means of delivering quality language services prior to limiting services due to resource limitations.

APPENDIX C

Applicant STEP #2 - Required Questions Relating to Language Assistance Measures

Taking into account the four-factor analysis, please answer the following questions in the six areas of the table below. (**Do not** attempt to answer the questions until you have completed the four-factor analysis.) The Department understands that your responses will depend on the outcome of the four-factor analysis. The requirement to provide language assistance does not vary, but the measures taken to provide the assistance will necessarily differ from organization to organization.

1. IDENTIFICATION OF LEP PERSONS SERVED OR LIKELY TO BE ENCOUNTERED IN YOUR PROGRAM		
a. Do you make an effort to identify LEP persons served in your program? (One way to identify LEP persons served in your program is to collect data on ethnicity, race, and/or preferred language.)	Yes	No
b. Do you make an effort to identify LEP persons likely to be encountered in the population eligible for your program or service? (One way to identify LEP persons likely to be encountered is by examining external data sources, such as Census data)	Yes	No
c. Does you make an effort to use data to identify new and emerging population or community needs?	Yes	No
2. NOTICE OF AVAILABILITY OF LANGUAGE ASSISTANCE		
Do you inform all applicants / clients of their right to receive language / communication assistance services at no cost? (Or, do you have procedures in place to notify LEP applicants / clients of their right to receive assistance, if needed?) <u>Example:</u> One way to notify clients about the availability of language assistance is through the use of an "I Speak" card.	Yes	No
3. STAFF TRAINING		
Do you provide training to personnel at all levels of your organization on federal civil rights laws compliance and the procedures for providing language assistance to LEP persons, if needed?	Yes	No
4. PROVISION OF LANGUAGE ASSISTANCE		
Do you provide language assistance to LEP persons, free of charge, in a timely manner? (Or, do you have procedures in place to provide language	Yes	No

APPENDIX C

assistance to LEP persons, if needed) In general, covered entities are required to provide two types of language assistance: (1) oral interpretation and (2) translation of written materials. Oral interpretation may be carried out by contracted in-person or remote interpreters, and/or bi-lingual staff. <u>(Examples</u> of written materials you may need to translate include vital documents such as consent forms and statements of rights.)		
5. ENSURING COMPETENCY OF INTERPRETERS USED IN PROGRAM AND THE ACCURACY OF TRANSLATED MATERIALS		
a. Do you make effort to assess the language fluency of all interpreters used in your program to determine their level of competence in their specific field of service? (Note: A way to fulfill this requirement is to use certified interpreters only.)	Yes	No
b. As a general rule, does your organization avoid the use of family members, friends, and other untested individual to provide interpretation services?	Yes	No
c. Does your organization have a policy and procedure in place to handle client requests to use a family member, friend, or other untested individual to provide interpretation services?	Yes	No
d. Do you make an effort to verify the accuracy of any translated materials used in your program (or use only professionally certified translators)? (Note: Depending on the outcome of the four-factor analysis, N/A (Not applicable) may be an acceptable response to this question.	Yes	No
6. MONITORING OF SERVICES PROVIDED		
Does you make an effort to periodically evaluate the effectiveness of any language assistance services provided, and make modifications, as needed?	Yes	No
If there is a designated staff member who carries out the evaluation function? If so, please provide the person's title: <hr/>	Yes	No

By signing and submitting this attachment to RFA# _____, the Contractor affirms that it:

- 1.) Has completed the four-factor analysis as part of the process for creating its proposal, in response to the above referenced RFA.

APPENDIX C

- 2.) Understands that Title VI of the Civil Rights Act of 1964 requires the Contractor to take reasonable steps to ensure meaningful access to ***all*** LEP persons to all programs, services, and/or activities offered by my organization.
- 3.) Understands that, if selected, the Contractor will be required to submit a detailed description of the language assistance services it will provide to LEP persons to ensure meaningful access to programs and/or services, within 10 days of the date the contract is approved by Governor and Council.

Contractor/Vendor Signature

Contractor's Representative Name/Title

Contractor Name

Date



APPENDIX D

Price Schedule	
New Hampshire Department of Health and Human Services	
Vendor Name: _____ Services: <u>State Disbursement Unit Services</u>	

PRICE PER ITEM (FROM JANUARY 1, 2021 THROUGH JUNE 30, 2026)

Deliverable		Qty.	1/1/21 - 6/30/21	7/1/21 - 6/30/22	7/1/22 - 6/30/23	7/1/23 - 6/30/24	7/1/24 - 6/30/25	7/1/25 - 6/30/26
1.	Remittance Processing Services							
	a. EFT payments							
	i. Regular							
	ii. Research							
	iii. Suspense							
	b. Coupon Payments							
	i. All							
	c. Data-Entered Payments							
	i. Other than research and suspense							
	ii. Research							
	iii. Suspense							
2.	Disbursement Processing Services							
	a. Check Writing							
	b. Provision for Deliveries (Check Pulls)							
3.	Banking Service							
	a. Monthly Cost							
	b. NSF Tracking							

**New Hampshire Department of Health and Human Services
State Disbursement Unit (SDU) Services**



Deliverable			Qty.	1/1/21 - 6/30/21	7/1/21 - 6/30/22	7/1/22 - 6/30/23	7/1/23 - 6/30/24	7/1/24 - 6/30/25	7/1/25 - 6/30/26
	c.	NSF Check Handling							
4.	Printing and Mailing Services								
	a.	Monthly Obligor Coupons							
	b.	Labels							
	c.	Weekly Employer Coupons							
5.	Other Costs and Services								
	a.	Provision for Daily Reporting							
	b.	Provision for Post Office Box Rental							
	c.	Employer Terminations							
	d.	Imaging							
	e.	Imaging (EFT)							
	f.	Provision for Deliveries (non-processable)							
6.	Debit Card - <i>Costs to BCSS</i>								
	a.	Deposit Notification							
	b.	ATM Withdrawal Fee							
	c.	Cash Withdrawal @Teller							
	d.	Cash-back with Purchase							
	e.	ATM Cash Withdrawal International							
	f.	ATM Balance Inquiry							
	g.	ATM Denial							
	h.	Teller Withdrawal							
	i.	POS Signature Transaction							
	j.	POS PIN Based Transaction							

**New Hampshire Department of Health and Human Services
State Disbursement Unit (SDU) Services**



Deliverable			Qty.	1/1/21 - 6/30/21	7/1/21 - 6/30/22	7/1/22 - 6/30/23	7/1/23 - 6/30/24	7/1/24 - 6/30/25	7/1/25 - 6/30/26
	k.	Card Replacement							
	l.	Expedited Card Replacement							
	m.	Interactive Voice Response							
	n.	Renewal Card Issuance							
	o.	Monthly Statement							
	p.	Overdraft Fee							
	q.	Web Account							
	r.	90 Days Funds Returned to State if card not delivered or card is not activated							
7.	Debit Card - <i>Costs to Cardholder</i>								
	a.	Deposit Notification							
	b.	ATM Withdrawal Fee							
	c.	Cash Withdrawal @Teller							
	d.	Cash-back with Purchase							
	e.	ATM Cash Withdrawal International							
	f.	ATM Balance Inquiry							
	g.	ATM Denial							
	h.	Teller Withdrawal							
	i.	POS Signature Transaction							
	j.	POS PIN Based Transaction							
	k.	Card Replacement							
	l.	Expedited Card Replacement							

**New Hampshire Department of Health and Human Services
State Disbursement Unit (SDU) Services**



Deliverable			Qty.	1/1/21 - 6/30/21	7/1/21 - 6/30/22	7/1/22 - 6/30/23	7/1/23 - 6/30/24	7/1/24 – 6/30/25	7/1/25 – 6/30/26
	m.	Interactive Voice Response							
	n.	Renewal Card Issuance							
	o.	Monthly Statement							
	p.	Overdraft Fee							
	q.	Web Account							
	r.	90 Days Funds Returned to State if card not delivered or card is not activated							
8.	SSAE No. 16								
9.	Other Costs (please specify)								

**New Hampshire Department of Health and Human Services
State Disbursement Unit (SDU) Services**



PRICE PER ITEM (FROM JULY 1, 2026 THROUGH DECEMBER 31, 2031)

Deliverable		Qty.	7/1/26 – 6/30/27	7/1/27 – 6/30/28	7/1/28 – 6/30/29	7/1/29 – 6/30/30	7/1/30 – 6/30/31	7/1/31 – 12/31/31
1.	Remittance Processing Services							
	a. EFT payments							
	i. Regular							
	ii. Research							
	iii. Suspense							
	b. Coupon Payments							
	i. All							
	c. Data-Entered Payments							
	i. Other than research and suspense							
	ii. Research							
	iii. Suspense							
2.	Disbursement Processing Services							
	a. Check Writing							
	b. Provision for Deliveries (Check Pulls)							
3.	Banking Service							
	a. Monthly Cost							
	b. NSF Tracking							
	c. NSF Check Handling							
4.	Printing and Mailing Services							
	a. Monthly Obligor Coupons							
	b. Labels							
	c. Weekly Employer Coupons							
5.	Other Costs and Services							
	a. Provision for Daily Reporting							

**New Hampshire Department of Health and Human Services
State Disbursement Unit (SDU) Services**



Deliverable			Qty.	7/1/26 – 6/30/27	7/1/27 – 6/30/28	7/1/28 – 6/30/29	7/1/29 – 6/30/30	7/1/30 – 6/30/31	7/1/31 – 12/31/31
	b.	Provision for Post Office Box Rental							
	c.	Employer Terminations							
	d.	Imaging							
	e.	Imaging (EFT)							
	f.	Provision for Deliveries (non-processable)							
6.	Debit Card - <i>Costs to BCSS</i>								
	a.	Deposit Notification							
	b.	ATM Withdrawal Fee							
	c.	Cash Withdrawal @Teller							
	d.	Cash-back with Purchase							
	e.	ATM Cash Withdrawal International							
	f.	ATM Balance Inquiry							
	g.	ATM Denial							
	h.	Teller Withdrawal							
	i.	POS Signature Transaction							
	j.	POS PIN Based Transaction							
	k.	Card Replacement							
	l.	Expedited Card Replacement							
	m.	Interactive Voice Response							
	n.	Renewal Card Issuance							
	o.	Monthly Statement							

**New Hampshire Department of Health and Human Services
State Disbursement Unit (SDU) Services**



Deliverable			Qty.	7/1/26 – 6/30/27	7/1/27 – 6/30/28	7/1/28 – 6/30/29	7/1/29 – 6/30/30	7/1/30 – 6/30/31	7/1/31 – 12/31/31
	p.	Overdraft Fee							
	q.	Web Account							
	r.	90 Days Funds Returned to State if card not delivered or card is not activated							
7.	Debit Card - <i>Costs to Cardholder</i>								
	a.	Deposit Notification							
	b.	ATM Withdrawal Fee							
	c.	Cash Withdrawal @Teller							
	d.	Cash-back with Purchase							
	e.	ATM Cash Withdrawal International							
	f.	ATM Balance Inquiry							
	g.	ATM Denial							
	h.	Teller Withdrawal							
	i.	POS Signature Transaction							
	j.	POS PIN Based Transaction							
	k.	Card Replacement							
	l.	Expedited Card Replacement							
	m.	Interactive Voice Response							
	n.	Renewal Card Issuance							
	o.	Monthly Statement							
	p.	Overdraft Fee							
	q.	Web Account							
	r.	90 Days Funds Returned to State if card not							

**New Hampshire Department of Health and Human Services
State Disbursement Unit (SDU) Services**



Deliverable			Qty.	7/1/26 – 6/30/27	7/1/27 – 6/30/28	7/1/28 - 6/30/29	7/1/29 - 6/30/30	7/1/30 – 6/30/31	7/1/31 – 12/31/31
		delivered or card is not activated							
8.	SSAE No. 16								
9.	Other Costs (please specify)								



APPENDIX E

Program Staff List				
Vendor Name:				
Services: State Disbursement Unit Services				
Position Title	Current Individual in Position	Full Time Equivalent	Minimum Qualifications (specify education and experience)	Required Certifications and Licenses
*Please list which site(s) each staff member works at if your organization has multiple sites.				



APPENDIX F

Required Data Elements for Billing Coupons

1. The following information, as provided by BCSS or newly designed by the selected Vendor as approved by BCSS, must be printed on the monthly bill/coupon (Form 684) for Direct Pay cases:
 - 1.1. Case Identification Number
 - 1.2. Payor Social Security Number
 - 1.3. Payor Name
 - 1.4. Payor Address
 - 1.5. BCSS District Office
 - 1.6. BCSS District Office Address
 - 1.7. Child Support Worker Name and Telephone Number
 - 1.8. Amount due for current support
 - 1.9. Amount due for arrears
 - 1.10. Total amount due for month
 - 1.11. Payee Name
 - 1.12. Last payment processed
 - 1.13. Current payment
 - 1.14. Past due payment/arrearage as of billing date
 - 1.15. Billing date
 - 1.16. Blank spaces to enter address change or other information
 - 1.17. Policy Release (PR) number (thirteen (13) digits)
 - 1.18. Policy release date (up to five (5) digits)
 - 1.19. Information relative to returned checks including minimum payment due, amount of payment enclosed, payment due date and check number
 - 1.20. OCR line for Payor ID Number (eight (8) digits)
 - 1.21. OCR line for minimum amount due (up to twelve (12) digits, including cents)
 - 1.22. OCR line for due date of payment
 - 1.23. Blank space for the amount of payment enclosed
 - 1.24. Blank space for the check number of the payment
2. The following information, as provided by BCSS or newly designed by the selected Vendor as approved by BCSS, must be printed on the monthly bill/coupon for Income Withholding Coupon cases:
 - 2.1. Case Identification Number
 - 2.2. Payor Social Security Number



- 2.3. Payor Name
- 2.4. Payor Address
- 2.5. BCSS District Office
- 2.6. BCSS District Office Address
- 2.7. Child Support Worker Name and Telephone Number
- 2.8. Amount due for current support
- 2.9. Amount due for arrears
- 2.10. Total amount due for month
- 2.11. Payee Name
- 2.12. Last payment processed
- 2.13. Current payment
- 2.14. Past due payment/arrearage as of billing date
- 2.15. Billing date
- 2.16. Blank spaces to enter address change or other information
- 2.17. Policy Release (PR) number (thirteen (13) digits)
- 2.18. Policy release date (up to five (5) digits)
- 2.19. Information relative to returned checks including minimum payment due, amount of payment enclosed, payment due date and check number
- 2.20. OCR line for Payor ID Number (eight (8) digits)
- 2.21. OCR line for minimum amount due (up to twelve (12) digits, including cents)
- 2.22. OCR line for due date of payment
- 2.23. Blank space for the amount of payment enclosed
- 2.24. Blank space for the check number of the payment
- 2.25. Spaces provided for Employers to enter:
 - 2.25.1. Actual amount withheld
 - 2.25.2. Check Number (*)
 - 2.25.3. Last ten (10) digits
3. The following check-off boxes (in separate tear-off section if in paper form) must be printed on the monthly bill/coupon for Income Withholding Coupon cases to capture wage termination data:
 - 3.1. Termination date (with spaces for Employer to enter effective date)
 - 3.2. Resigned/Quit/Retired data (with spaces for Employer to enter effective date)
 - 3.3. Fired date (with spaces for Employer to enter effective date)
 - 3.4. Never worked here



- 3.5. Address change / comments
- 3.6. Also include in above section, provided to the Contractor by BCSS, are the following:
 - 3.6.1. DO code (pre-printed)
 - 3.6.2. Employer Name (pre-printed)
 - 3.6.3. Employer NEN (pre-printed)
 - 3.6.4. Employer Name (pre-printed)
 - 3.6.5. Remittance ID (pre-printed)
4. On the reverse side of the Income Withholding Coupon, the following information as provided by BCSS or newly designed by the selected Vendor as approved by BCSS, must be printed:
 - 4.1. Statutory authority for completing the form (New Hampshire RSA 458:B-6)
 - 4.2. Instructions for completing the form
 - 4.3. All District Office Names
 - 4.4. All District Office Telephone Numbers
 - 4.5. All District Office Fax Numbers
 - 4.6. All District Office Code Numbers



APPENDIX G

SDU Information Technology Provisions Statement of Work

1. TECHNOLOGY REQUIREMENTS

Appendix H Technical Requirements Checklist contains mandatory technical requirements for this technology solution and vendor services. Vendors shall complete the Technical Requirements Checklist in accordance with the instructions on the "Instructions" tab of Appendix H.

2. TESTING AND ACCEPTANCE

In its proposal, the Vendor is to include its proposed Test Plan methodology and any scheduling assumptions used regarding the customer resource efforts required during User Acceptance Testing. After Contract award, the Vendor will be required to customize its proposed Test Plan methodology to reflect the needs of the Project and include the details of its Test Plan methodology in the detailed Work Plan (the first Project Deliverable).

In addition, the Vendor will provide a mechanism for reporting actual test results vs. expected results and for the resolution and tracking of all errors and problems identified during test execution. The Vendor will also provide training as necessary to the State staff responsible for test activities.

2.1. Testing Requirements

All testing and acceptance addressed herein shall apply to testing the Technology Solution. This shall include planning, test scenario development, Data, and system preparation for testing, and support of State staff during execution of Acceptance Testing (UAT).

2.2. Test Planning and Preparation

The overall Test Plan will guide all testing. The Vendor provided, State approved, Test Plan will include, at a minimum, identification, preparation, and documentation of planned testing, a requirements traceability matrix, test variants, test scenarios, test cases, test scripts, test data, test phases, expected results, and a tracking method for reporting actual versus expected results as well as all errors and problems identified during test execution.

It is crucial that customer training and testing activities not be abbreviated in order to meet project implementation schedules. Therefore, the State requires that the testing activities be represented both in terms of effort and duration.

Vendors must disclose in their proposals the scheduling assumptions used in regard to the State resource efforts during testing.

State testing will commence upon the Vendor Project Manager's certification, in writing, that the Vendor's own staff has successfully executed all prerequisite Vendor testing, along with reporting the actual testing results, prior to the start of any testing executed by State staff.

The State will commence its testing within five (5) business days of receiving certification from the Vendor that the State's personnel have been trained and the Technology Solution is installed, configured, complete, and ready for State testing. The



testing will be conducted by the State in an environment independent from the Vendor's development environment. The Vendor must assist the State with testing in accordance with the Test Plan and the Work Plan, utilizing test and live data to validate data and reports, at no additional cost.

2.3. Testing Schedule

Testing begins upon completion of the Technology Solution configuration as required and user training according to the Work Plan. Testing ends upon issuance of a letter of UAT Acceptance by the State.

Vendor must demonstrate that their testing methodology can be integrated with the State standard methodology described below:

2.3.1. Unit Testing

- 2.3.1.1. Application components are tested on an individual basis to verify that the inputs, outputs, and processing logic of each application component functions without errors. Unit Testing is performed in either the development environment or a testing environment.
- 2.3.1.2. The goal is to find errors in the smallest unit of Software. If successful, subsequent integration testing should only reveal errors related to the integration between application components.

2.3.2. System Integration Testing

- 2.3.2.1. Validates the integration between the individual unit application components and verifies that the new System meets defined requirements and supports execution of interfaces and business processes. The Systems Integration Test is performed in a test environment.
- 2.3.2.2. Emphasizes end-to-end business processes and the flow of information across applications. It includes all key business processes and interfaces being implemented, confirms Data transfers with external parties, and includes the transmission or printing of all electronic and paper documents.
- 2.3.2.3. The State will conduct System Integration Testing, utilizing scripts developed, as identified in the Test Plan, to validate the functionality of the System and its interfaces. The State will also use System Integration Testing to validate modifications, fixes and other System interactions with the Vendor supplied Software Solution.

2.3.3. Conversion /Migration Validation Testing

- 2.3.3.1. The Conversion/Migration Validation Testing should replicate the entire flow of the converted Data through the Software Solution. As the Software Solution is interfaced to legacy or third-party applications, the testing verifies that the resulting converted legacy Data performs correctly.



2.3.4. Installation Testing

- 2.3.4.1. Application components are installed in the System test environment to test the installation routines and are refined for the eventual production environment. This activity serves as a dry run of the installation steps in preparation for configuring the production System.

2.3.5. User Acceptance Testing (UAT)

- 2.3.5.1. The User Acceptance Test (UAT) is a Verification process performed in a copy of the production environment. The User Acceptance Test verifies System functionality against predefined Acceptance criteria that support the successful execution of approved business processes.
- 2.3.5.1.1. The Vendor's Project Manager must certify in writing, that the Vendor's own staff has successfully executed all prerequisite Vendor testing, along with reporting the actual testing results prior to the start of any testing executed by State staff.
- 2.3.5.1.2. The State will be presented with a State approved Test Plan, test scenarios, test cases, test scripts, test Data, and expected results, as well as written Certification of the Vendor's having completed the prerequisite tests, prior to the State staff involvement in any testing activities.
- 2.3.5.1.3. UAT will also serve as a performance and stress test of the System. It may cover any aspect of the new System, including administrative procedures such as backup and recovery. The results of the UAT provide evidence that the new System meets the User Acceptance criteria as defined in the Work Plan.
- 2.3.5.2. Upon successful conclusion of UAT and successful System deployment, the State will issue a letter of UAT Acceptance and the respective Warranty Period shall commence.

2.3.6. Performance Tuning and Stress Testing

- 2.3.6.1. Vendor shall develop and document hardware and Software configuration and tuning of System infrastructure as well as assist and direct the State's System Administrators and Database Administrators in configuring and tuning the infrastructure to support the Software throughout the Project.
- 2.3.6.2. Scope
- 2.3.6.2.1. The scope of performance testing shall measure the system level metrics critical for the development of the applications infrastructure and operation of the applications in the production environment. It will include the measurement of response rates of the application for end-user transactions and resource



- utilization (of various servers and network) under various load conditions. These response rates shall become the basis for changes and retesting until optimum system performance is achieved.
- 2.3.6.2.2. The application transactions shall be identified with specific roles and selected transactions shall be recorded for the performance measurements. These will be compared to baselines to determine if object and/or system performance increases as changes are made.
- 2.3.6.2.3. Performance testing shall consider the full scope of the application infrastructure with emphasis on the most heavily used or shared transactions. Performance testing of the application will profile the identified user transactions and assist in the identifying performance gaps to improve the most critical parts of the applications.
- 2.3.6.2.4. Performance testing and tuning shall occur in the final production environment and shall use a copy of the final production database to provide the best results.
- 2.3.6.2.5. Vendor must lead this effort. Responsibilities include identifying appropriate tunable parameters and their default and recommended settings, developing scripts, which accurately reflect business load and coordinating reporting of results.
- 2.3.6.3. Test Types
- 2.3.6.3.1. Performance testing shall use two different types of tests to determine the stability of the application. They are baseline tests and load tests.
- 2.3.6.4. Baseline Test: Baseline tests shall collect performance Data and load analysis by running scripts where the output is broken down into business transactions or functions. The test is like a single user executing a defined business transaction. During baseline testing, each individual script is run to establish a baseline for transaction response time, throughput and other user-based metrics. Usually each business transaction is executed multiple times during a single test run to obtain an average for the user-based metrics required for the performance testing evaluations. It must be noted that changes made to the code after baseline testing is completed will skew the results collected to date. All effort will be made to provide a code test base that is tested in the environment for problems prior to the establishment of the baseline, which are used in future testing and tuning efforts. Any changes introduced into the environment after performance testing has started can compromise the accuracy of the results and will force a decision to be made whether baseline results need to be recreated.



- 2.3.6.5. Load Tests: Load testing will determine if the behavior of a system can be sustained over a long period of time while running under expected conditions. Load tests helps to verify the ability of the application environment under different load conditions based on workload distribution. System response time and utilization is measured and recorded.
- 2.3.6.6. Tuning
 - 2.3.6.6.1. Tuning will occur during both the development of the application and load testing. Tuning is the process whereby the application performance is maximized. This can be the result of making code more efficient during development as well as making tuning parameter changes to the environment.
 - 2.3.6.6.2. For infrastructure tuning, parameters will be identified for all components prior to undertaking the load testing efforts. This should include a list of the variables, their definitions, the default settings, range of acceptable settings and the settings as testing begins. This will permit the team to identify the areas of most potential gain and a starting point. Tuning is a process which is repeated until the team feels that the systems are running at or near optimum performance.
- 2.3.6.7. Implementing Performance and Stress Test: Performance and Stress test Tools must be provided by the Vendor for this effort. Consideration must be given to licensing with respect to continued use for Regression Testing. If the Vendor is familiar with open source low/no cost tools for this purpose those tools should be identified in your response.
- 2.3.6.8. Scheduling Performance and Stress Testing:
 - 2.3.6.8.1. Vendor shall perform test planning. The steps for planning include identification of application functionality as well as what percentage of normal daily use is represented by each function. This information will become the foundation for scripting so that tests closely represent what loads in production will look like.
 - 2.3.6.8.2. Vendor shall provide definition and expectations from testing. This definition should include who is in charge of testing and coordinating results, anticipated run times, logs required for tracking, their locations and which technician is responsible to track and provide them following each test to the team.
 - 2.3.6.8.3. Initial test runs shall be completed to establish that the tests and Data sets can be run to completion without errors. The ratio of types of transactions which



- makeup the test shall be reviewed prior to the beginning of testing and then again once testing has begun to make sure that testing accurately reflects the system performing in production.
- 2.3.6.8.4. Initial tests shall be used to establish a baseline from which all subsequent tests will be compared. Tests will be considered for baseline status once two of them have been run within 2% of each other in key and overall performance areas. No changes to the test scripts or Data sets (with the exception of restores after each test) can be done to the test environment once tuning has begun so as to not damage the comparison to baseline results. The systems must be restarted prior to each test run to assure all cache is cleaned out. All effort will be made to run these tests at a time when system and network infrastructure utilization doesn't impact the results. Tests will be run in close proximity to our infrastructure to eliminate the public network from our environment.
- 2.3.6.8.5. Post test reporting and result assessment will be scheduled following each test. The team will compare these results to the baseline and a determination must be made to make additional changes to the parameter being tuned or return to the prior configuration and select another parameter to tune while keeping in mind that significant changes to any one parameter may require the retesting of some others. Careful work on identifying dependencies up front should minimize this impact.
- 2.3.6.8.6. If Defects are identified in the application during testing, they will be recorded; however, changes to the application code should be avoided if possible so as not to affect baseline comparisons. If a change to the application is required new baselines will be established (and possibly the execution of prior tests to validate changes with the new application) before testing can continue.
- 2.3.6.8.7. When performing capacity testing against a GUI the focus will be on the ability of the interface to respond to user input.
- 2.3.6.8.8. During stress/load testing the tester will attempt to stress or load an aspect of the system to the point of failure. The goal being to determine weak points in the system architecture. The tester will identify peak load conditions at which the program will fail to handle required processing loads within required time spans.



- 2.3.6.8.9. During Performance testing the tester will design test case scenarios to determine if the system meets the stated performance criteria (i.e. A Login request shall be responded to in 1 second or less under a typical daily load of 1000 requests per minute.). In both cases, the tester will determine the capacity of the system under a known set of conditions.

2.3.6.9. Regression Testing

- 2.3.6.9.1. As a result, of the user testing activities, problems will be identified that require correction. The State will notify the Vendor of the nature of the testing failures in writing. The Vendor will be required to perform additional testing activities in response to State and/or user problems identified from the testing results.

- 2.3.6.9.2. Regression Testing means selective re-testing to detect faults introduced during the modification effort, both to verify that the modifications have not caused unintended adverse effects, and to verify that the modified and related (possibly affected) System components still meet their specified requirements.

- 2.3.6.9.2.1. For each minor failure of an Acceptance Test, the Acceptance Period shall be extended by corresponding time defined in the Test Plan.

- 2.3.6.9.2.2. The Vendor shall notify the State no later than five (5) business days from the Vendor's receipt of written notice of the test failure when the Vendor expects the corrections to be completed and ready for retesting by the State. The Vendor will have up to five (5) business days to make corrections to the problem unless specifically extended in writing by the State.

- 2.3.6.9.2.3. When a programming change is made in response to a problem identified during user testing, a Regression Test Plan should be developed by the Vendor based on the understanding of the program and the change being made to the program. The Test Plan has two objectives:

- 2.3.6.9.2.3.1. Validate that the change/update has been properly incorporated into the program; and
 - 2.3.6.9.2.3.2. Validate that there has been no unintended change to the other portions of the program.



- 2.3.6.9.2.4. The Vendor will be expected to:
 - 2.3.6.9.2.4.1. Create a set of test conditions, test cases, and test data that will validate that the change has been incorporated correctly;
 - 2.3.6.9.2.4.2. Create a set of test conditions, test cases, and test data that will validate that the unchanged portions of the program still operate correctly; and
 - 2.3.6.9.2.4.3. Manage the entire cyclic process.
- 2.3.6.9.2.5. The Vendor will be expected to execute the Regression Test, provide actual testing results, and certify its completion in writing to the State prior to passing the modified Software application to the users for retesting.
- 2.3.6.10. In designing and conducting such Regression Testing, the Vendor will be required to assess the risks inherent to the modification being implemented and weigh those risks against the time and effort required for conducting the Regression Tests. In other words, the Vendor will be expected to design and conduct Regression Tests that will identify any unintended consequences of the modification while taking into account Schedule and economic considerations.
- 2.3.6.11. In their Proposals Vendors must acknowledge their responsibilities for regression testing as described in this section.
- 2.3.7. Security Review and Testing
 - 2.3.7.1. IT Security involves all functions pertaining to the securing of State Data and Systems through the creation and definition of security policies, procedures and controls covering such areas as Identification, Authentication and non-repudiation.
 - 2.3.7.2. All components of the Software shall be Reviewed and tested to ensure they protect the State's hardware and Software and its related Data assets.



Table 1

Service Component	Defines the set of capabilities that:
Identification and Authentication	Supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users.
Access Control	Supports the management of permissions for logging onto a computer or network.
Encryption	Supports the encoding of Data for security purposes
Intrusion Detection	Supports the detection of illegal entrance into a computer system.
Verification	Supports the confirmation of authority to enter a computer system, application or network.
Digital Signature	Guarantees the unaltered state of a file.
User Management	Supports the administration of computer, application and network accounts within an organization.
Role/Privilege Management	Supports the granting of abilities to users or groups of users of a computer, application or network.
Audit Trail Capture and Analysis	Supports the identification and monitoring of activities within an application or system.
Input Validation	Ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.

2.3.7.3. In their Proposal, the Vendors must acknowledge their responsibilities for security testing. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability. Tests shall, at a minimum, cover each of the service components. Test procedures shall include 3rd party Penetration Tests (pen test) or code analysis and review.

2.3.7.4. Prior to the System being moved into production, the Vendor shall provide results of all security testing to the Department of Information Technology for Review and Acceptance. All Software and hardware shall be free of malicious code (malware).

2.3.8. Penetration Testing

2.3.8.1. Implement a methodology for penetration testing that includes the following:

- 2.3.8.1.1. Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115);
- 2.3.8.1.2. Includes coverage for the entire CDE perimeter and critical systems;
- 2.3.8.1.3. Includes testing from both inside and outside the network;
- 2.3.8.1.4. Includes testing to validate any segmentation and scope-reduction controls;



- 2.3.8.1.5. Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in PCI DSS Compliance: Requirement 6.5;
- 2.3.8.1.6. Defines network-layer penetration tests to include components that support network functions as well as Operating Systems;
- 2.3.8.1.7. Includes Review and consideration of threats and vulnerabilities experienced in the last 12 months; and
- 2.3.8.1.8. Specifies retention of penetration testing results and remediation activities results.
- 2.3.8.2. Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
- 2.3.8.3. Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade a sub-network added to the environment, or a web server added to the environment).
- 2.3.8.4. Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections
- 2.3.8.5. If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are Operational and effective, and isolate all out-of-scope systems from in-scope systems.

3. TRANSITION PROJECT MANAGEMENT

3.1. Transition Work Plan

In the event that the State must transition operations to a new service provider, a Transition Phase will be required to establish the State as a new customer and implement the Technology Solution and operational procedures. Vendor shall submit a preliminary Work Plan in their Proposals. The Work Plan shall include, without limitation, a detailed description of the Schedule, tasks, Deliverables, major milestones, task dependencies, and payment schedule. A final Work Plan may be incorporated into the resultant contract, at the State's discretion, prior to Governor and Executive Council approval, or at minimum, may be due five (5) business days after Contract award upon approval by Governor and Executive Council.

The Vendor shall update the Work Plan as necessary but no less than every two weeks to accurately reflect the status of the Project, including without limitation, the Schedule, tasks, Deliverables, major milestones, task dependencies, and payment schedule. Any updates to the Work Plan shall require the written approval of the State prior to final incorporation into the Contract.

Unless otherwise agreed in writing by the State, changes to the Work Plan shall not relieve the Vendor from liability to the State for any damages resulting from the Vendor's failure to perform its obligations under the Contract, including without limitation, performance in accordance with the Schedule.



In the event of a delay in the Schedule, the Vendor must immediately notify the State in writing. The written notification will identify the nature of the delay, i.e., specific actions or inactions of the Vendor or State causing the problem; its estimated duration period to reconciliation; specific actions that need to be taken to correct the problem; and the expected Schedule affect the Project.

In the event the Vendor requires additional time to correct Deficiencies, the Schedule shall not change unless previously agreed in writing by the State, except that the Schedule shall automatically extend on a day-to-day basis to the extent that the delay does not result from Vendor's failure to fulfill its obligations under the Contract. To the extent that the State's execution of its major tasks takes longer than described in the Work Plan, the Schedule shall automatically extend on a day-to-day basis.

Notwithstanding anything to the contrary, the State shall have the option to terminate the Contract for default, at its discretion, if it is dissatisfied with the Vendor's Work Plan or elements within the Work Plan.

3.2. Transition Meetings and Reports

During the Transition Phase, if applicable, the Vendor shall conduct several required meetings to facilitate communications.

Kickoff Meeting: Participants will include the State and Vendor Project Team and major stakeholders. This meeting is to establish a sound foundation for activities that will follow.

Status Meetings: Participants will include, at the minimum, the Vendor Project Manager and the State Project Manager. These meetings will be conducted at least bi-weekly and address overall Project status and any additional topics needed to remain on schedule and within budget.

Status Reports: A status and issue report from the Vendor shall serve as the basis for discussion. The Work Plan must be reviewed at each status meeting and updated, at minimum, on a bi-weekly basis, in accordance with the Contract.

4. GENERAL TERMS

4.1. Licenses

If a license is included as a component of the Technology Solution, the Vendor must include a copy of the software license in the Proposal for the State's consideration.

4.1.1. Title

The Vendor must hold the right to allow the State to use the software or hold all title, right, and interest (including all ownership and intellectual property rights) in the software and its associated documentation.

4.2. Warranty

4.2.1. System

The Vendor shall warrant that the Technology Solution must operate to conform to the specifications, terms, and requirements of the Contract.



4.2.2. Non-Infringement

The Vendor shall warrant that it has good title to, or the right to allow the State to use all Services, equipment, and software provided under this Contract, and that such services, equipment, and software ("Material") do not violate or infringe any patent, trademark, copyright, trade name or other intellectual property rights or misappropriate a trade secret of any third party.

4.2.3. Viruses, Destructive Programming

The Vendor shall warrant that the software will not contain any viruses, destructive programming, or mechanisms designed to disrupt the performance of the software.

4.2.4. Compatibility

The Vendor shall warrant that all System components, including any replacement or upgraded System software components provided by the Vendor to correct deficiencies or as an enhancement, shall operate with the rest of the System without loss of any functionality.

4.2.5. Professional Services

The Vendor shall warrant that all services provided under the Contract will be provided in a professional manner in accordance with industry standards and that services will comply with performance standards.

4.2.6. Warranty Period

The warranty period shall extend for the duration of the Contract and any extensions, with the exception of the warranty for non-infringement, which shall extend indefinitely.

4.3. State-Owned Documents and Data

The Vendor shall provide the State access to all documents, State data, materials, reports, and other work in progress relating to the Contract ("State Owned Documents"). Upon expiration or termination of the Contract with the State, Vendor shall turn over all State-owned documents, State data, material, reports, and work in progress relating to this Contract to the State at no additional cost to the State. State-Owned Documents must be provided in their original format.

4.4. Intellectual Property

Upon successful completion and/or termination of the implementation of the Project, the Vendor shall own and hold all title, rights and interest in any software modifications (Custom Code) developed in connection with performance of obligations under the Contract, or modifications to the Vendor provided software, and their associated documentation, including any and all performance enhancing operational plans and the Vendor's special utilities. The Vendor shall license back to the State the right to produce, publish, or otherwise use such software, source code, object code, modifications, reports, and documentation developed under the Contract.

In no event shall the Vendor be precluded from developing, for itself or for others, materials that are competitive with or similar to custom software or modifications developed in connection with performance of obligations under the Contract. In addition, the Vendor shall be free to use its general knowledge, skills, experience, and any other ideas, concepts, know-how, and techniques that are acquired or used in the course of its performance under this Contract.



4.5. Contingency Plan/Disaster Recovery Plan

It is critical to the smooth operation of the NH SDU that downtime be minimized. The Vendor must present a written disaster recovery plan. The disaster recovery plan must include a sample test scenario.

- 4.5.1. Current versions of any software associated with NH SDU operations must be running at all times.
- 4.5.2. A daily backup file of the NH SDU database must be stored at a secure site away from the NH SDU and specifically designed for this type of secure record storage. This site must be accessible to the State. The backup cycle must be a month in length.
- 4.5.3. Vendor must identify a "hot site" for payment processing in case of a disaster at the NH SDU location. Payment processing at the "hot site" must be described in detail.
- 4.5.4. The Vendor must conduct a disaster recovery exercise annually.
- 4.5.5. Payment processing must not be interrupted for more than 72 hours following any disaster.

4.6. End of Contract Transition Plan

As noted previously, the Contract will be for five (5) years, and may be extended for up to an additional five (5) years, contingent upon satisfactory performance by the Vendor, supporting funding, and Governor and Executive Council approval. The Vendor must explain how it plans to handle the transition to a new vendor.

- 4.6.1. The State will inform the Vendor thirty (30) calendar days in advance of the routine termination of the Contract. The Vendor agrees to participate in an orderly transition.
- 4.6.2. All data in the SDU Database is the property of the State of New Hampshire. The Vendor will transfer to the State all data contained in the SDU database and all records related to functions performed and payments processed during the term of their Contract. The current Vendor will supply the State with the images of all financial instruments received and processed during the term of their Contract. The State will make this information available to the new vendor.
- 4.6.3. If a contract extension for up to six months is needed to affect an orderly transition, the Vendor must agree to do so. The terms and conditions of the Contract then in place shall prevail during this extension period.
- 4.6.4. The new vendor will have no responsibility for any unidentified payments posted by the previous contractor.
- 4.6.5. The SDU Vendor shall supply the following items to the State, except where the NH SDU Vendor does not have the right to transfer such items to a third party:
 - 4.6.5.1. The NH SDU database, including the structure, all data models, data dictionaries, drawings, graphic representations, specifications and file formats within the NH SDU System, including all hardware and software required to operate the NH SDU System.



- 4.6.5.2. NH SDU network configuration diagrams, maintenance logs, and security provisions.
- 4.6.6. Below we describe those end-of-contract transfer provisions that are required regardless of which course of action is chosen by the State.
 - 4.6.6.1. In those instances where the Vendor does not have the right to transfer hardware or software to the State, the Vendor shall provide the State with the name and version of the software necessary to make the Vendor's technical solution fully functional.
 - 4.6.6.2. The Vendor shall supply to the State, on the next day following termination of services under this Contract, all data and information stored in the SDU database and in all other Vendor databases and information systems (including backup copies in any medium located at the SDU site and in off-site storage). The format and medium in which the data and information are supplied shall be specified by the State.

5. NARRATIVE TOPICS FOR MANDATORY NARRATIVE RESPONSES

This section provides a series of topics related to the proposed Technology Solution that the State will consider for selecting the SDU solution.

Topic	Page Limit	Point Value
5.1 Operational Topics		
5.1.1. Topic 1 – Data Exchange	Page Limit – 2	35 Points
5.1.2. Topic 2 – System Security and Hosted Environment	Page Limit – 6	35 Points
5.1.3. Topic 3 – Back-up and Recovery	Page Limit – 2	35 Points
5.1.4. Topic 4 – Assurance of Business Continuity	Page Limit – 2	35 Points
5.2 Transition Topics		
5.2.1. Topic 5 – Transition and Implementation Services	Page Limit – None	35 Points
5.2.2. Topic 6 – User Acceptance Testing	Page Limit – 3	35 Points
5.2.3. Topic 7 – Assurance of Business Continuity	Page Limit – 2	35 Points
5.2.4. Topic 8– Project Management	Page Limit – 2	35 Points
5.2.5. Topic 9– Risk and Issue Management	Page Limit – 2	35 Points
5.2.6. Topic 10 – Transition Work Plan	Page Limit – None	35 Points

5.1. Operational Topics

5.1.1. Topic 1 – Data Exchange

Response Page Limit: 2

Provide a detailed description of the mechanisms and tools included in the proposed System to enable the specified data sharing between the Vendor and the State.



- 5.1.1.1. Describe the transmission of customer and EFT data within the system to financial institutions and the State. Address frequency, workflow, and technology.

5.1.2. Topic 2 - System Security and the Hosted Environment

Response Page Limit: 6

Provide a detailed description of the security design and architectural features incorporated into the proposed System. At a minimum, discuss the following:

- 5.1.2.1. Describe the business practices and technology employed to ensure that your system and staff comply with:
- Payment Card Institute (PCI) standards;
 - National Automated Clearing House Association (NACHA) security standards.
- 5.1.2.2. Describe the System assurance provisions incorporated into the proposed System. At a minimum, discuss the following:
- What process or methodology is employed within the proposed System to ensure data integrity?
- 5.1.2.3. Discuss your company's practices pertaining to the following security testing:
- The identification and authentication methods used to ensure that users and any interfacing applications are identified and that their identities are properly verified.
 - The authorization methods used to ensure that users and customer applications can only access data and services for which they have been properly authorized.
 - The immunity methods used to ensure that unauthorized malicious programs (e.g., viruses, worms and Trojan horses) do not infect the application.
 - The methods used to ensure that communications and data integrity are not intentionally corrupted via unauthorized creation, modification or deletion.
 - The methods used to ensure that the parties to interactions with the application cannot later repudiate or rebut those interactions.
 - The intrusion detection methods used to ensure the detection, recording and review of attempted access or modification by unauthorized individuals.
 - The privacy methods used to ensure that confidential data and sensitive communications are kept private.
 - The System maintenance methods used to ensure that unauthorized System maintenance does not unintentionally disrupt the security mechanisms of the application or supporting hardware.
 - The testing methods conducted to load and stress test your System to determine its ability to withstand Denial of Service (DoS) attacks.



- Your software patch schedule employed to protect the software from new security vulnerabilities as they arise.
- The ability of your System's software to be installed in a "locked-down" fashion so as to turn off unnecessary features (user accounts, operating System services, etc.) thereby reducing the software's security vulnerabilities and attack surfaces available to System hackers and attackers.

5.1.3. Topic 3 – Backup and Recovery

Response Page Limit: 2

Provide a detailed description of the backup and recovery processes used to protect mission-critical Data.

5.1.3.1. The State seeks a sound backup and recovery provision as part of the Solution. Describe the tools used for backup and recovery of applications and data. Describe the impact of the proposed backup process on the operation of the System. Also, address the following:

- Use of and method for logging and journalizing;
- Single points of failure and recommended approaches for their elimination; and
- Approach to redundancy.

5.1.4. Topic 4 – Assurance of Business Continuity

Response Page Limit: 2

Provide a detailed description of the disaster recovery and business continuity plans that mitigates risk to the State.

5.1.4.1. Vendors are asked to provide information on their disaster recovery and business continuity plans in the event that their systems and human resources site become unavailable.

5.1.4.2. Payment processing at the "hot site" must be described in detail.

5.2. Transition Topics

In the event that that State needs to transition disbursement operations to a new vendor, a well-planned implementation will be critical. The following topics address the transition phase of the engagement.

5.2.1. Topic 5 – Transition and Implementation Services

Response Page Limit: None

Provide a detailed description of transition services required to establish operations for the State of New Hampshire.

5.2.1.1. The response must include a description of the following:

- Describe the implementation of the technology and business processes;
- Include a graphic workflow of the process;
- Identify timeframes for performing implementation milestones;
- The resources to be employed, including both State and Vendor by milestone;
- Roles and responsibilities of State and Vendor staff;



- The time commitment required for both State and Vendor resources;
- The communication plan to be employed;
- A detailed summary of the specific Deliverables;
- Describe the handling of State data during the transition phase; and
- Provide a sample of a transition plan that you have developed for other clients.

5.2.2. Topic 6 – User Acceptance Testing

Response Page Limit: 3

Provide a detailed description of the support the Vendor will supply to assist the State during user acceptance testing of the configured technology solution for New Hampshire.

5.2.2.1. State staff will conduct data validation and User Acceptance Testing, but support from the selected Vendor is required. To define the type of support that will be provided, address the following questions:

- Describe your testing methodology and include a proposed test plan.
- How much time should the State allow to complete User Acceptance Testing of a component?
- What support will be provided to prepare State staff during Acceptance Testing?
- How will members of the testing team be prepared to test the configured software?
- What Documentation of configured software will be available to the testing team?
- Based on experience in similar projects, how many and what types of Defects are likely to be encountered in User Acceptance Testing? (Include metrics from other projects to support this response.)
- How quickly will a suspected Defect be investigated, and what classifications are planned for suspected Defects?
- How quickly will Defects, if any, be corrected?
- Provide a sample User Acceptance Test Plan from a completed project as an appendix.

5.2.3. Topic 7 – Business Continuity

Response Page Limit: 2

Provide a detailed description of your business continuity plan that mitigates risk to the State.

5.2.3.1. Vendors are asked to provide information on their business continuity plan in the event that their hosting site becomes unavailable.

5.2.3.2. Discuss necessary planning for moving operations to a remote site if the hosting site is incapacitated.



- 5.2.3.3. What is the recovery time objective and how will your company continue to meet federally required response metrics?
- 5.2.3.4. The State believes that additional software license fees solely related to redundancy for assurance of business continuity would be inappropriate. If the Proposal differs from this standard, describe and provide rationale for the difference.

5.2.4. Topic 8 – Project Management

Response Page Limit: 2

Provide a detailed description of project management reporting.

- 5.2.4.1. The State believes that effective communication and reporting are essential to the success of the transition. Describe the planned project management activities as they pertain to the three phases: Planning, Implementation, and Operations.

Describe how the following will be managed:

- Introductory Meeting;
- Kickoff Meeting;
- Status Meetings;
- Status Reports;
- The Work Plan;
- Letter of Acceptance; and
- Change Order Process.

- 5.2.4.2. As an appendix, provide an example of status reports prepared for another similar project. Names of the project and of any individuals involved may be removed.

5.2.5. Topic 9 – Risk and Issue Management

Response Page Limit: 2

Provide a detailed description of the proposed approach to timely identification and effective action on issues and risks.

- 5.2.5.1. Describe the proposed approach to managing risks and issues. Include a sample tracking document.
- 5.2.5.2. Highlight the methodology to ensure that State staff is involved in the process.
- 5.2.5.3. Provide a description of known risks and proposed steps to mitigate them.

5.2.6. Topic 10 – Transition Work Plan

Response Page Limit: None

Provide a preliminary Work Plan for the Planning and Implementation Phases of the engagement. The Vendor's preliminary proposed Work Plan shall include: a description of the schedule, tasks, Deliverables, major milestones, task dependencies, and a payment schedule. The Work Plan shall also address resource allocations (both State and Vendor team members).



- 5.2.6.1. Provide a preliminary Work Plan depicting tasks, task dependencies, schedule, milestones, Deliverables, and payment schedule. Define both proposed written and software Deliverables. Include sufficient detail that the State will be able to identify departures from the Work Plan in sufficient time to seek corrective action. In particular, provide information about staffing.
- 5.2.6.2. Describe all Deliverables to be produced in the Project. Ensure that all Deliverables and milestones are identified in the Work Plan. Identify and discuss the following:
 - All assumptions upon which the Work Plan is based;
 - Descriptions of recommended roles by activity and time required for both State and Vendor members of the Project Team;
 - Assignments of members of the Vendor's team identified by role to specific tasks; and
 - Critical success factors for the Project.
- 5.2.6.3. Discuss how this Work Plan will be used and State access to Plan details including resource allocation. Also, discuss frequency for updating the Plan weekly and for every status meeting. Explain how the State will know whether the Project is on schedule and within budget.

Contractor Instructions for Business (BR) and Technical (TR) Requirements	
<p>Contractor Response Column:</p> <p>the current release of the software can fully support ALL the functionality described in the row, without special customization. A "Yes" can only be used if the delivery method is Standard (see delivery method instructions below). Otherwise, enter an "No"; A "No" can only be used with delivery method Future, Custom, or Not Available/Not Proposing (see delivery method instructions below).</p>	Place a "Yes" if
<p>Criticality Column:</p> <p>(M) Indicates a requirement that is "Mandatory". The State considers it to be of such great importance that it must be met in order for the proposal to be accepted. If the proposer believes that there is something about their proposal that either obviates the need for this requirement or makes it of less importance this must be explained within the comments. The State retains the right to accept a proposal if the need of the requirement is reduced or eliminated by another feature of the proposal.</p> <p>(P) Indicates a requirement which is "Preferred". This requirement is considered by the State to be of great usefulness but the lack of this feature is not considered serious enough to disqualify the proposal.</p> <p>(O) Indicates a requirement which is "Optional". This requirement is considered by the State to be one which useful or potentially useful but not a central feature of the Project.</p>	
<p>Delivery Method Column:</p> <p>Complete the delivery method using a Standard, Future, Custom, or Not Available/Not Proposing (as defined below) that indicates how the requirement will be delivered.</p> <p>Standard - Feature/Function is included in the proposed system and available in the current software release.</p> <p>Future - Feature/Function will be available in a future release. (Provide anticipated delivery date, version, and service release in the comment area.)</p> <p>Custom - Feature/Function can be provided with custom modifications. (Respondent must provide estimated hours and average billing rate or flat cost for the software modification in the comment area. These cost estimates should add up to the total cost for software modifications found in the cost summary table in Section X of the RFP).</p> <p>Not Available/Not Proposing - Feature/Function has not been proposed by the Contractor. (Provide brief description of why this functionality was not proposed.)</p>	
<p>Comments Column:</p> <p>For all Delivery Method responses Contractors must provide a brief explanation of how the requirement will be met. Free form text can be entered into this column.</p>	
Contractor Instructions for Activity, Deliverable, and Milestone	
Contractor shall complete the Activity Deliverable, and Milestone Table identifying estimated delivery date and price.	

APPLICATION REQUIREMENTS					
State Requirements			Contractor		
Req #	Requirement Description	Criticality	Contractor Response	Delivery Method	Comments
GENERAL SPECIFICATIONS					
A1.1	Ability to access data using open standards access protocol (please specify supported versions in the comments field).	M			
A1.2	Data is available in commonly used format over which no entity has exclusive control, with the exception of National or International standards. Data is not subject to any copyright, patent, trademark or other trade secret regulation.	M			
A1.3	Web-based compatible and in conformance with the following W3C standards: HTML5, CSS 2.1, XML 1.1	M			
APPLICATION SECURITY					
A2.1	Verify the identity or authenticate all of the system client applications before allowing use of the system to prevent access to inappropriate or confidential data or services.	M			
A2.2	Verify the identity and authenticate all of the system's human users before allowing them to use its capabilities to prevent access to inappropriate or confidential data or services.	M			
A2.3	Enforce unique user names.	M			
A2.4	The Contractor Solution should enforce complex passwords for Administrator Accounts in accordance with DoIT's statewide User Account and Password Policy. The Contractor solution must allow for comprehensive auditing, tracking and access logging of the special accounts created for activities such as 'production testing and debugging.	M			
A2.5	Enforce the use of complex passwords for general users using a mix of capital letters, lower-case letters, numbers, special characters, minimum length of eight characters and prohibit the use of personal information.	M			
A2.6	Encrypt passwords in transmission and at rest within the database.	M			
A2.7	Establish ability to expire passwords after a definite period of time in accordance with DoIT's statewide User Account and Password Policy	M			
A2.8	Provide the ability to limit the number of people that can grant or change authorizations	M			
A2.9	Establish ability to enforce session timeouts during periods of inactivity.	M			
A2.10	The application shall not store authentication credentials or sensitive data in its code.	M			

A2.11	<p>Logs must be configured using "fail-safe" configuration. Audit logs must contain the following minimum information:</p> <ol style="list-style-type: none"> 1. User IDs (of all users who have access to the system) 2. Date and time stamps 3. Changes made to system configurations 4. Addition of new users 5. New users' level of access 6. Files accessed (including users) 7. Access to systems, applications and data 8. Access trail to systems and applications (successful and unsuccessful attempts) 9. Security events 	M			
A2.12	The application shall log all activities to a central server to prevent parties to application transactions from denying that they have taken place.	M			
A2.13	All logs must be kept for 10 years.	M			
A2.14	The application must allow a human user to explicitly terminate a session. No remnants of the prior session should then remain.	M			
A2.15	Do not use Software and System Services for anything other than they are designed for.	M			
A2.16	The application Data shall be protected (encrypted) from unauthorized use when at rest	M			
A2.17	The application shall keep any sensitive Data or communications private from unauthorized individuals and programs.	M			
A2.18	Subsequent application enhancements or upgrades shall not remove or degrade security requirements	M			
A2.19	Utilize change management documentation and procedures	M			
A2.20	Web Services : The service provider shall use Web services exclusively to interface with the State's data in near real time when possible.	M			
A2.21	Application must have the capability to search all information including log search and playback.	M			
A2.22	Application must provide Role-based access control to all system features and data, including specified data elements.	M			
A2.23	Application must have Multi-Factor Authentication.	M			

A2.24	Contractor must perform patching and corrections to mitigate security vulnerabilities of a critical nature within three Business Days and those of a major nature within 10 Business Days. The Department will determine the level of criticality in consultation with the system Contractor.	M			
A2.25	Contractor must be compatible with multiple standard browsers in accordance to the State's IT Standards. The solution shall allow access from standard browsers without requiring specialized plug-ins or applets to function. The solution shall allow for a mobile app that is available through standard IOS and Android App Stores.	M			
A2.26	Contractor must ensure that device firmware and version is up to date and updates are not disruptive to the user experience.	M			
A2.27	Contractor shall install and update all server patches updates and other utilities within 60 days of release from the manufacturer.	M			

TESTING					
State Requirements			Contractor		
Req #	Requirement Description	Criticality	Contractor Response	Delivery Method	Comments
APPLICATION SECURITY TESTING					
T1.1	All components of the Software shall be reviewed and tested to ensure they protect the State's web site and its related Data assets.	M			
T1.2	The Contractor shall be responsible for providing documentation of security testing, as appropriate. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability.	M			
T1.3	Provide evidence that supports the fact that Identification and Authentication testing has been recently accomplished; supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users	M			
T1.4	Test for Access Control; supports the management of permissions for logging onto a computer or network	M			
T1.5	Test for encryption; supports the encoding of data for security purposes, and for the ability to access the data in a decrypted format from required tools.	M			
T1.6	Test the Intrusion Detection; supports the detection of illegal entrance into a computer system	M			
T1.7	Test the Verification feature; supports the confirmation of authority to enter a computer system, application or network	M			
T1.8	Test the User Management feature; supports the administration of computer, application and network accounts within an organization.	M			
T1.9	Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network	M			
T1.10	Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system	M			
T1.11	Test Input Validation; ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.	M			
T.1.12	For web applications, ensure the application has been tested and hardened to prevent critical application security flaws. (At a minimum, the application shall be tested against all flaws outlined in the Open Web Application Security Project (OWASP) Top Ten (http://www.owasp.org/index.php/OWASP_Top_Ten_Project))	M			

Appendix H - Technical Requirements

T1.13	Provide the State with validation of 3rd party security reviews performed on the application and system environment. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review (please specify proposed methodology in the comments field).	M			
T1.14	Prior to the System being moved into production, the Contractor shall provide results of all security testing to the Department of Information Technology for review and acceptance.	M			
T1.15	Contractor shall provide documented procedure for migrating application modifications from the User Acceptance Test Environment to the Production Environment.	M			
STANDARD TESTING					
T2.1	The Contractor must test the software and the system using an industry standard and State approved testing methodology.	M			
T2.2	The Contractor must perform application stress testing and tuning.	M			
T2.3	The Contractor must provide documented procedure for how to sync Production with a specific testing environment.	M			
T2.4	The Contractor must define and test disaster recovery procedures.	M			

Appendix H - Technical Requirements

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Contractor		
Req #	Requirement Description	Criticality	Contractor Response	Delivery Method	Comments
OPERATIONS					
H1.1	Contractor shall provide an ANSI/TIA-942 Tier 3 Data Center or equivalent. A tier 3 data center requires 1) Multiple independent distribution paths serving the IT equipment, 2) All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture and 3) Concurrently maintainable site infrastructure with expected availability of 99.982%	M			
H1.2	Contractor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application, log and audit trail requirements and support users with permission based logins.	M			
H1.3	The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access shall only be granted to those with a need to perform tasks in the Data Center.	M			
H1.4	Contractor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.	M			
H1.5	Contractor shall monitor System, security, and application logs.	M			
H1.6	Contractor shall manage the sharing of data resources.	M			
H1.7	Contractor shall manage daily backups, off-site data storage, and restore operations.	M			
H1.8	The Contractor shall monitor the availability of their application.	M			
H1.9	Remote access shall be customized to the State's business application. In instances where the State requires access to the application or server resources not in the DMZ, the Contractor shall provide remote desktop connection to the server through secure protocols such as a Virtual Private Network (VPN).	M			
H1.10	The Contractor shall report any breach in security in conformance with DHHS Information Security Requirements (Exhibit K).	M			

Appendix H - Technical Requirements

H1.11	The Contractor will provide a completed Security Audit Report prior to contract execution. The Security Audit Report must include a SOC 2 Report with certification.	M			
H1.12	The Contractor will provide a completed Security Audit Report with results to the Department each year. The Security Audit Report must include a SOC 2 Report with certification.	M			
DISASTER RECOVERY					
H2.1	Contractor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs.	M			
H2.2	The disaster recovery plan shall identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems shall offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services however, these failed components will have to be replaced.	M			
H2.3	Contractor shall adhere to a defined and documented back-up schedule and procedure.	M			
H2.4	Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.	M			
H2.5	Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.	M			
H2.6	Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.	M			
H2.7	Data recovery – In the event that recovery back to the last backup is not sufficient to recover State Data, the Contractor shall employ the use of database logs in addition to backup media in the restoration of the database(s) to afford a much closer to real-time recovery. To do this, logs must be moved off the volume containing the database with a frequency to match the business needs.	M			
HOSTING SECURITY					

Appendix H - Technical Requirements

H3.1	The Contractor shall employ security measures ensure that the State's application and data is protected.	M			
H3.2	If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.	M			
H3.3	All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection.	M			
H3.4	All components of the infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability.	M			
H3.5	The Contractor shall ensure its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.	M			
H3.6	The Contractor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Contractor' hosting infrastructure and/or the application upon request.	M			
H3.7	All servers and devices must have event logging enabled. Logs must be protected with access limited to only authorized administrators. Logs shall include System, Application, Web and Database logs.	M			
H3.8	Operating Systems (OS) and Databases (DB) shall be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA	M			
H3.9	The Contractor shall notify the State's Project Manager of any security breaches within two (2) hours of the time that the Contractor learns of their occurrence.	M			
H3.10	The Contractor shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.	M			

SERVICE LEVEL AGREEMENT

Appendix H - Technical Requirements

H4.1	The Contractor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M			
H4.2	The Contractor shall maintain the hardware and Software in accordance with the specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M			
H4.3	The Contractor shall repair or replace the hardware or software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M			
H4.4	All hardware and software components of the Contractor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers.				
H4.5	The State shall have unlimited access, via phone or Email, to the Contractor technical support staff between the hours of 7:00am to 5:00pm Monday through Friday EST.	M			
H4.6	<p>The Contractor shall conform to the specific deficiency class as described:</p> <ul style="list-style-type: none"> o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service. 	M			

Appendix H - Technical Requirements

H4.7	As part of the maintenance agreement, ongoing support issues shall be responded to according to the following: a. Class A Deficiencies - The Contractor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Contractor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State shall notify the Contractor of such Deficiencies during regular business hours and the Contractor shall respond back within four (4) hours of notification of planned corrective action; The Contractor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract.	M			
H4.8	The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M			
H4.9	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M			
H4.10	If The Contractor is unable to meet the uptime requirement, The Contractor shall credit State's account in an amount based upon the following formula: $(\text{Total Contract Item Price}/365) \times \text{Number of Days Contract Item Not Provided}$. The State must request this credit in writing.	M			
H4.11	The Contractor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M			
H4.12	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M			

Appendix H - Technical Requirements

H4.13	The Contractor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M			
H4.14	The Contractor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M			

Appendix H - Technical Requirements

SUPPORT & MAINTENANCE REQUIREMENTS					
State Requirements			Contractor		
Req #	Requirement Description	Criticality	Contractor Response	Delivery Method	Comments
SUPPORT & MAINTENANCE REQUIREMENTS					
S1.1	The Contractor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M			
S1.2	Maintain the hardware and Software in accordance with the Specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M			
S1.3	Repair Software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M			
S1.4	The State shall have unlimited access, via phone or Email, to the Contractor technical support staff between the hours of 7:00am to 5:00pm- Monday through Friday EST.	M			
S1.5	<p>The Contractor response time for support shall conform to the specific deficiency class as described below or as agreed to by the parties:</p> <ul style="list-style-type: none"> o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service. 	M			

S1.6	The Contractor shall make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.	M			
S1.7	For all maintenance Services calls, The Contractor shall ensure the following information will be collected and maintained: 1) nature of the Deficiency; 2) current status of the Deficiency; 3) action plans, dates, and times; 4) expected and actual completion time; 5) Deficiency resolution information, 6) Resolved by, 7) Identifying number i.e. work order number, 8) Issue identified by.	P			
S1.8	The Contractor must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) identification of repeat calls or repeat Software problems.	P			
S1.9	As part of the Software maintenance agreement, ongoing software maintenance and support issues, shall be responded to according to the following or as agreed to by the parties: a. Class A Deficiencies - The Contractor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Contractor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State shall notify the Contractor of such Deficiencies during regular business hours and the Contractor shall respond back within four (4) hours of notification of planned corrective action; The Contractor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract; or as agreed between the parties	M			
S1.10	The Contractor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M			
S1.11	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M			

Appendix H - Technical Requirements

S1.12	The Contractor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: All change requests implemented; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M			
S1.13	The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M			
S1.14	The Contractor will guide the State with possible solutions to resolve issues to maintain a fully functioning, hosted System.	M			
S1.15	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M			
S1.16	The Contractor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M			
S1.17	All hardware and software components of the Contractor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers.	M			
S1.18	The Contractor shall provide the State with a personal secure FTP site to be used by the State for uploading and downloading files if applicable.	M			



APPENDIX I Physical Security Requirements

1. During the period of performance of the Contract, the selected Vendor must comply with all physical security requirements that are mandated by federal and/or state laws, rules, or regulations. The selected Vendor must comply with the Physical Security requirements included in Appendix G SDU IT Provisions.
2. The selected Vendor must permit access to the SDU by agents of the State or federal government for the purpose of ascertaining compliance with all applicable laws, rules, regulations and the conditions of the Contract.
3. The selected Vendor must make every effort to protect the SDU from damage by accident, theft, malicious intent, fire, loss of utilities, environmental hazards such as flood and hurricanes, vandalism, and unauthorized access.
4. The selected Vendor must maintain restricted access to the SDU, and that the SDU is located in a self-contained area that only performs SDU functions.
5. The SDU processing center shall have security doors, and a locking system for all doors such as card key locks, or push button code type locks.
6. All employees shall enter and exit the SDU through one access point and visitors' entry shall be controlled at the main entrance reception station. All visitors to the facility shall be required to register at the reception area and shall be escorted by SDU personnel.
7. The SDU shall have floor to ceiling walls, or walls that are at least eight (8) feet high and joined to a ceiling made of impenetrable steel, expanded steel mesh or similar material.
8. The selected Vendor must limit access to the SDU processing center to the following: SDU processing center staff, appropriate and authorized accounting and management staff employed by the selected Vendor, authorized subcontractors, auditors designated by the selected Vendor, federal and state auditors, DCSS staff and other authorized by the Director of DCSS.
9. All SDU employees who have access to or control over funds collected under the child support enforcement program shall be covered by a bond against loss resulting from employee dishonesty. (Refer to 45 CFR 302.19.)
10. All payment processing activities that involve financial instruments and all other payment processing activities including but not limited to the opening of the mail, shall take place within the SDU processing center.
11. At all times when work in accordance with this contract is being performed, there shall be no fewer than two (2) people in the SDU, one of whom shall be a supervisor. A security camera shall monitor all business operations within the SDU.
12. The SDU processing center shall have a fireproof, immovable safe for safeguarding processed financial instruments until transported to the bank for deposit.
13. All SDU employees shall work at desks without drawers and all personal belongings shall be kept outside the SDU.



APPENDIX J

Required Data Elements for Payment Processing

Data elements required in the processing of collections for all direct pay payments from payors, Wage Assignment payments, District Office payments, Out-of-State payments and State Tax Intercept are as follows:

<u>Type</u>	<u>Elements</u>
Direct pay from payors	Case ID Number Amount Enclosed Check Number (*) Date of receipt at SDU
Wage Assignment/Income Withholding	Case ID number Amount paid Check number (*) Date of receipt at DO (Form 681 or Form 697)
District Office	Case ID number Amount paid Check number (*) Date of receipt at DO (Form 681 or Form 697)
Out of State/Out of State Tax Intercept	Case ID Number Payment amount Check number (*) Date of receipt or check date as provided by the other State

*The last ten (10) digits of check number are required for processing.



APPENDIX K

Statement on Standards for Attestation Engagements (SSAE 16)

No later than forty (40) working days after the end of each NH State Fiscal Year on June 30, the selected Vendor must provide the Department of Health and Human Services a "SOC 1" Type 2 report in accordance with the American Institute of Certified Public Accountants, Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. The report will assess the design of internal controls and their operating effectiveness. The reporting period must cover the previous twelve (12) months or the entire period since the previous reporting period. The Department will share the entire report with internal and external auditors of the State of New Hampshire and federal oversight agencies.

1. The selected Vendor must provide assurances to the State that the service auditor will be selected through a competitive procurement process to perform audit services for the selected Vendor on contractual engagements where SSAE No.16, Statement on Standards for Attestation Engagements, type audits are either required or appropriate.
2. The selected Vendor must retain the services of a certified public accounting firm, to perform annual SSAE No. 16, Statement on Standards for Attestation Engagements, audits of the New Hampshire State Disbursement Unit. On-site portions of the annual service audit all be scheduled, performed and completed prior to the end of a State Fiscal Year ending June 30. A draft service audit report for the applicable State Fiscal Year must be delivered to BCSS no later than fifteen (15) working days after the end of the applicable State Fiscal Year on June 30. A final Service Auditor's Report must be delivered to BCSS no later than forty (40) working days after the end of the applicable State Fiscal Year on June 30.
3. The selected Vendor will require the service auditor to perform an audit that conforms to SSAE-No.16, (Statement on Standards for Attestation Engagements) in strict compliance to the methods and standards for a Type II review based on criteria established by the American Institute of Certified Public Accountants.
4. BCSS will provide data and information pertaining to State Disbursement Unit operations and/or controls that are necessary for the completion of the Service Auditor's Report to the service auditor.
5. The selected Vendor must supervise, coordinate, and facilitate the service auditor's conduct of the SSAE-No.16 audit.
6. The services auditor will bear final responsibility for the content and findings of the Service Auditor's Report.
7. Service Auditor's Report. The SSAE No.16 Type 2 Service Auditor's Report must include:
 - 7.1. Description by the service organization's management of its system of policies and procedures for providing services to user entities, including control objectives and related controls as they relate to the services provided, throughout the specified period of time.
 - 7.2. Written assertion by the service organization's management about whether:
 - 7.2.1. The aforementioned description fairly presents the system in all material respects;



- 7.2.2. The controls were suitably designed to achieve the control objectives stated in that description; and
 - 7.2.3. The controls operated effectively throughout the specified period to achieve those control objectives.
- 7.3. Report of the service organization's auditor, which:
 - 7.3.1. Expresses an opinion on the matters covered in management's written assertion; and
 - 7.3.2. Includes a description of the auditor's tests of operating effectiveness of controls and the results of those tests.
- 8. The service auditor's procedure must include, but are not limited to, the following:
 - 8.1. Obtaining information on the description of controls for the report through discussions with appropriate selected Vendor personnel, through reference to various forms of documentation, including, but not limited to system flow charts and narratives and through the performance of tests of controls.
 - 8.2. Determining whether the description provides sufficient information for user auditors to obtain an understanding of those aspects of the selected Vendor's controls that may be relevant to the Department's and BCSS' internal controls, including:
 - 8.2.1. The control environment, including but not limited to hiring practices, and key areas of authority;
 - 8.2.2. Risk assessment, including those associated with processing specific transactions;
 - 8.2.3. Control activities, including procedures on modifications to software;
 - 8.2.4. Communications, including the way user transactions are initiated; and
 - 8.2.5. Control monitoring, including involvement of internal auditors.
 - 8.3. Examining evidence of whether controls have been placed in operation by:
 - 8.3.1. Inquiry of appropriate selected Vendor's management and staff; and
 - 8.3.2. Inspection of the selected Vendor's documents and records; and
 - 8.3.3. Observation of the selected Vendor's activities and operations.
 - 8.4. Performing appropriate tests of control to determine that they were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives were achieved during the State Fiscal Year audited.
 - 8.5. Determining that significant changes, in the selected Vendor's controls, which were implemented before the start of the service auditor's fieldwork, are included in the selected Vendor's description of the controls.



APPENDIX L

Corrective Action / Liquidated Damages Disclosure

Proposals shall contain a summary explanation of all corrective actions undertaken and/or liquidated damages awarded to a customer(s) or other entities and paid by the Vendor in the past five (5) years. The Bureau of Child Support Services shall have the right to inquire further regarding the corrective actions or liquidated damages, including contacting the client/customer of the Vendor involved. The Vendor shall execute any necessary releases, if required.

Customer/Entity Name Contact Information	Summary Explanation